Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Azerbaijan

COUNTRY Azerbaijan

INDUSTRY Banking & Digital Banking

LAST UPDATED 13 November 2026

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

Key takeaways

- Only a bank licensed by the Central Bank of the Republic of Azerbaijan (CBAR) may take deposits. A new bank needs at least AZN 50 million in capital and goes through a two-stage licence review.
- Banks may open accounts fully online. Since 30 March 2026, CBAR rules allow remote opening with a liveness check, a face match against the customer's photo in a state database, and an enhanced electronic signature.
- For a brand-new remote customer, the Financial Monitoring Service (the financial intelligence unit) also requires a live or recorded video, a database check and two-factor authentication, so a selfie alone is not enough.
- Remote onboarding is not available through a proxy or for non-resident companies. Banks that use cloud services must keep sensitive customer data stored in Azerbaijan.
- Banks report cash transactions and wire transfers of AZN 20,000 or more. From 1 January 2027, wire reporting also captures an individual's transfers (other than a sole proprietor's) once they pass AZN 50,000 in a calendar month.

Azerbaijan is open to digital banking, but only inside the licensed bank perimeter: the Law on Banks has no separate licence for digital-only banks, so a neobank either holds a banking licence or partners with a bank that does.

Two authorities matter most. CBAR licenses and supervises banks and is their anti-money laundering (AML) supervisor. The Financial Monitoring Service sets the customer due diligence and reporting rules that apply to every bank.

The biggest obstacle for a new entrant is the combination of an AZN 50 million capital floor and an onboarding stack that must integrate with state information systems, an enhanced electronic signature, live video and in-country data storage.

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 banks	Level	Official site
Central Bank of the Republic of Azerbaijan (CBAR)	Banking licences, prudential rules, account opening and remote onboarding rules, authentication and information security rules, AML supervision of financial institutions, administrative fines	National	cbar.az
Financial Monitoring Service	Financial intelligence unit; due diligence, risk and reporting rules; suspicious transaction criteria; can suspend transactions	National	fiu.gov.az
Ministry of Digital Development and Transport	Personal data authority (Presidential Decree No 361); since 2 June 2026 its National Cybersecurity Agency keeps the state register of personal data systems and examines data subjects' complaints	National	mincom.gov.az
State Tax Service under the Ministry of Economy	State register of legal entities, including beneficial owner data	National	taxes.gov.az
Deposit Insurance Fund	Compensates insured depositors of participating banks	National	adif.gov.az
MONEYVAL (Council of Europe)	Evaluates the AML and counter-terrorist financing regime against Financial Action Task Force (FATF) standards	Supranational	coe.int

2 Licensing and authorisation

Under the Law on Banks No 590-IIQ, banking activity requires a CBAR licence (article 3.1), and deposit-taking is reserved to banks, local branches of foreign banks and the national postal operator (article 3.2). CBAR alone issues and revokes banking licences and branch permits (article 6.1).

Two-stage review

CBAR decides on the initial application within 90 calendar days, or 180 days where foreign founders participate (article 8.4). The bank then has 180 days to pay in its capital, register, and build its governance, IT and security arrangements (article 8.9). The final application is reviewed within 30 calendar days (article 8.11). CBAR may check owners of qualifying holdings (10% or more), beneficial owners and officers for fitness and propriety, and the source of the bank's capital (article 7.2).

Capital

CBAR's Rules on calculation of bank capital and its adequacy set a minimum aggregate capital, and a minimum charter capital for new banks, of AZN 50 million (points 3.2 and 3.6). A Basel III capital structure with new buffers applies in full from 1 January 2027 `Adopted, full compliance 1 Jan 2027`.

3 AML, KYC and customer due diligence

Banks are financial institutions and obliged entities under article 1.1.8 of 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, supervised by CBAR (article 16.1.1). The Financial Monitoring Service's Rules on verification measures during customer due diligence and the application of new technologies (the FMS CDD Rules, 21 February 2023) give the detail.

When CDD applies

Before a business relationship; before occasional transactions of AZN 20,000 or more (including linked transactions); before occasional wire transfers; on suspicion; and when earlier data is doubtful (AML/CFT Law article 4.2). Anonymous accounts are prohibited (article 4.1).

Data collected

For individuals: full name, personal identification number (FİN), citizenship, residence, date of birth, contact details, employer and position, income sources, and the purpose and expected volume of the relationship (FMS CDD Rules 2.1.1).

Beneficial ownership

Identify the natural person with a significant participation (10% or more), then anyone controlling by other means, then senior management (AML/CFT Law articles 1.1.20 and 4.7). For corporate customers, banks send the beneficial owner data identified in CDD to the Financial Monitoring Service within 3 working days (article 11.11).

Ongoing CDD

Refresh data at least yearly for high-risk customers, every two years for medium risk, every three years for low risk, and continuously for politically exposed persons (FMS CDD Rules 8.1).

Beneficial owner data is now also filed in the state register of legal entities kept by the State Tax Service. Companies registered before Law No 175-VIIQD of 11 April 2025 file in phases: large businesses by 31 December 2025, medium by 30 June 2026, small by 31 December 2026 and micro businesses by 31 December 2027 (article 12.1), so register data for smaller corporate customers may be incomplete until then.

Enhanced and simplified due diligence

Enhanced measures apply to high-risk customers, politically exposed persons and their relatives and associates, and persons from countries named in FATF calls (FMS CDD Rules 5.2). Options include senior management approval, source of funds and wealth evidence, and requiring the first payment from an account in the customer's name at a bank with similar standards (5.3). Simplified measures are allowed only where risk is assessed as low (AML/CFT Law article 4.18) and never when an enhanced trigger is present (4.4). If CDD cannot be completed, the bank must not open the account and must report to the Financial Monitoring Service (AML/CFT Law article 4.14). Wire transfers must carry payer and payee information under CBAR's Rules on applying CDD to electronic transfers of funds (point 3.1).

Reporting

Report	Trigger	Deadline
Cash transaction	AZN 20,000 or more	3 working days after the transaction
Wire transfer	AZN 20,000 or more per transfer; from 1 Jan 2027 also each further transfer once an individual's monthly total exceeds AZN 50,000 (sole proprietors excluded)	3 working days

Suspicious transaction or attempt	Any amount	Per Financial Monitoring Service procedure (AML/CFT Law article 11.4)
Suspicious transaction held before execution	High-risk profile, AZN 200,000 or more, or a withdrawal from the account	Report immediately; do not execute for 2 working days unless cleared earlier
Foreign politically exposed persons	Any transaction, regardless of suspicion	3 working days
Sanctioned persons' assets; CDD refused or halted	Any amount	Immediately, by the end of the working day

Thresholds come from the Financial Monitoring Service decision of 27 April 2023 and its amendment of 21 April 2026 `Amendment effective 1 Jan 2027`. Records are kept for at least 5 years after the transaction or relationship ends (AML/CFT Law article 6), and customers must not be tipped off (article 11.10). Banks also need approved internal AML rules, a senior responsible officer, staff training and an independent audit (article 10.1); those offering remote opening must review the identification process at least yearly (CBAR remote opening Regulation, point 7.1).

4 Identity verification and onboarding

Identity is verified from the documents in the annex to the FMS CDD Rules: the identity card for Azerbaijani citizens; a foreign passport or Azerbaijani residence permit for foreigners; a stateless person's identity card or residence permit; and specific documents for military personnel, refugees and seafarers. Data must be verified from reliable, independent sources (AML/CFT Law article 4.4.1).

Remote account opening

CBAR's Regulation on remote opening of accounts (Decision No 44/5 of 16 December 2025) `In force since 30 Mar 2026` covers credit institutions, investment firms (including custody and margin accounts), the postal operator, payment institutions and e-money institutions.

Remote identification uses photo capture, video recording or a real-time video call (point 5.4), and requires:

- colour images with the face clearly visible and uncovered, and no other person present or assisting (5.5);
- software liveness detection with at least three actions in random order, analysing natural physiological reactions (5.7);
- software matching of the face to the customer's photograph in a state information system (5.8);
- end-to-end encryption of the session (5.10);
- application data confirmed, and the contract signed, with an enhanced electronic signature (4.2, 6.3 and 6.4).

The Regulation also requires verification under the FMS CDD Rules (point 4.4), and the AML/CFT Law gives the Financial Monitoring Service the power to set verification for new technologies (article 8.5). Those rules make four measures mandatory when a relationship is first established remotely: an enhanced electronic signature, a check against electronic databases or independent sources, strong customer authentication with two independent factors, and identity verification by real-time video call or video recording (7.1 and 7.2). A new remote customer therefore needs video; photo capture fits cases outside that rule, such as an existing customer the bank chooses to re-identify.

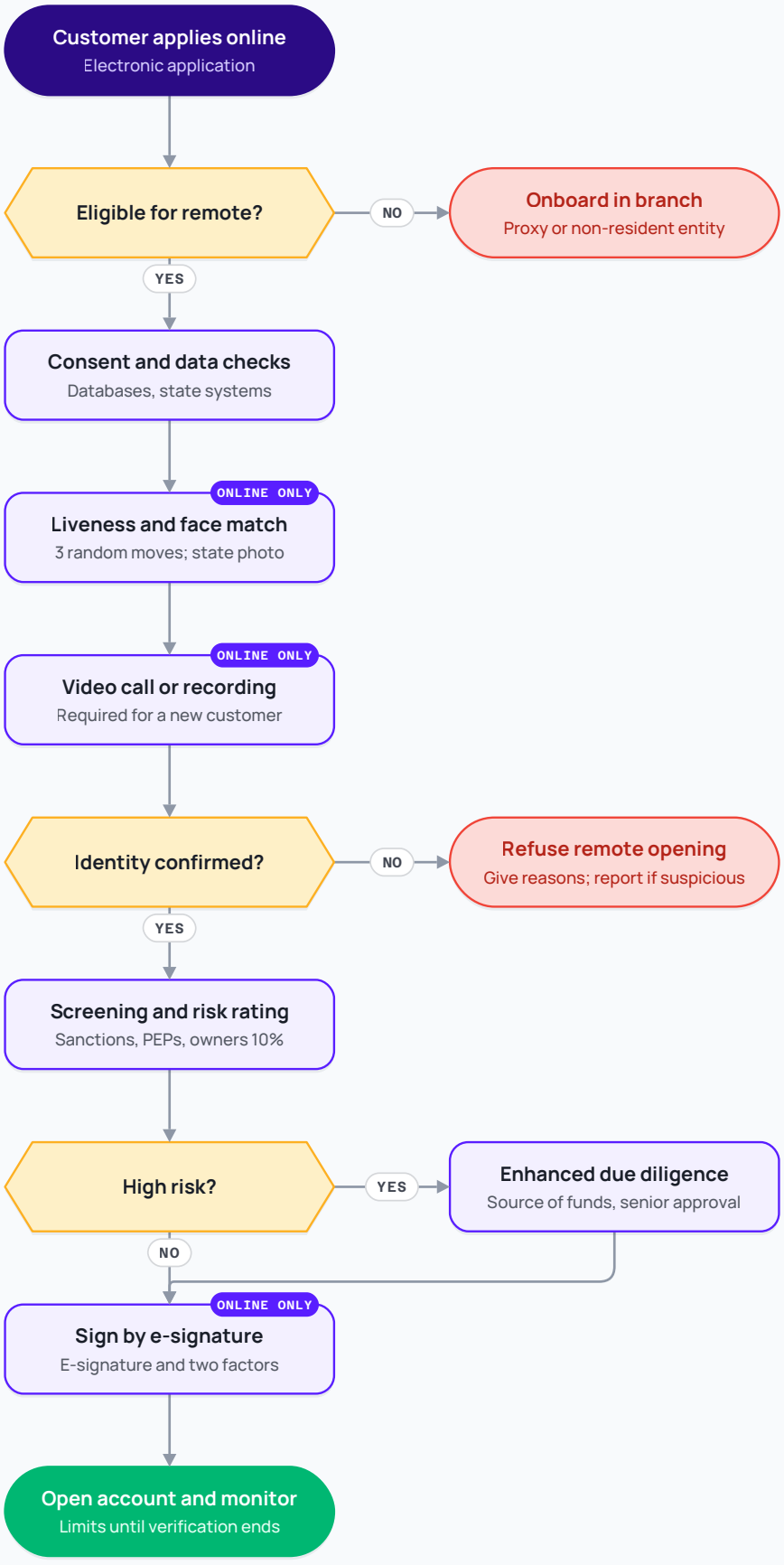


Figure 1. Remote account opening for a new individual customer at an Azerbaijani bank.

Reliance and existing customers

A bank may rely on CDD by another obliged entity but stays responsible, must obtain the data immediately, and must be able to get document copies by the end of the working day (AML/CFT Law article 5.1). Under the Regulation, data already held and kept current, obtained through reliance, or retrieved from integrated state information systems need not be resubmitted (point 4.3), and an existing customer opening a further account remotely need not be re-identified unless the bank judges it risky (5.9).

5 Digital channels: what's different

> **Bottom line:** remote account opening is fully permitted, but the rules prescribe the identity check itself: liveness, a face match to state records, video for new customers and an enhanced electronic signature.

Requirement	In person / branch	Online / remote	Difference
Permission to onboard	Account opening rules	Allowed under the remote opening Regulation (since 30 Mar 2026)	Differs
Risk treatment	Risk-based rating	Law treats new-technology relationships as high risk; remote channels listed as high-risk factors	Differs
Identity check	Identity document presented to staff	Liveness and state photo match; video for new customers	Differs
Signing	Handwritten signature	Enhanced electronic signature	Differs
Who may apply	Customer or authorised representative	Customer, parent, adoptive parent, guardian or a company's legal representative; no non-resident companies	Differs
Verification timing	Before the relationship	May finish within 5 working days, with usage limits meanwhile	Differs
Account access	In branch	Strong customer authentication with dynamic linking for remote payments	Differs

CDD data, reporting, sanctions	AML/CFT Law and FMS rules	Same rules	Same
Retention period	At least 5 years	At least 5 years, including video, audio, images and logs	Same

High risk by statute

Article 8.1 of the AML/CFT Law requires banks to treat relationships and transactions conducted through new technologies as high-risk, to assess those technologies before launch, and to abandon a technology that does not allow full CDD (article 8.6). The FMS CDD Rules turn this into risk factors: electronic and mobile banking, non-face-to-face channels, and cards ordered online and used through a mobile app may be classed as high-risk delivery channels (3.11).

Deferred verification with limits

For relationships established using new technologies, verification may be completed after the relationship starts, but within 5 working days (FMS CDD Rules 6.4), with limits on the number, type, amount and purpose of transactions until then (6.5). The Regulation also lets banks set limits on remotely opened accounts, provided the customer is told (point 3.3).

Authentication and opt-out

CBAR's Rules on application of strong customer authentication require two of knowledge, possession and inherence; for remote payments, elements dynamically linked to amount and payee; no more than 3 failed attempts before blocking; and idle sessions closed after 5 minutes in mobile apps or 30 minutes in internet banking (points 2.1 to 2.3). Customers may also block remote account opening in their name; the block can be lifted only in person (Regulation, point 3.4).

6 Data protection and biometrics

The Law on Personal Data No 998-IIIQ applies in full to biometric data, expressly including facial images, fingerprints, voice and signatures (article 9.5). Processing needs consent or a legal basis that defines its purposes and methods (article 9.6). The Ministry of Digital Development and Transport is the personal data authority; since 2 June 2026 its National Cybersecurity Agency registers personal data systems and handles complaints

(Presidential Decree No 676, Charter 3.1.24 and 3.1.25). The remote opening Regulation requires written consent to data processing before identification starts (point 5.2), systems that meet the Law on Personal Data (point 3.1), and retention of all data, video and audio files, images and logs created during identification (point 7.3).

7 Sector-specific obligations

Bank secrecy and consent to share

Banks guarantee secrecy of accounts, transactions and customer data (Law on Banks article 41.1). Information goes to third parties only with the customer's written consent in a separate document, signed by hand, by enhanced electronic signature, or by another method CBAR sets for remote account opening (article 41.2).

Cloud and third-party providers

CBAR's Requirements on information security in supervised entities `In force since 9 Apr 2025` require a supplier register and risk assessment (point 4.9). Cloud contracts must keep sensitive information, defined to include personal data and bank secrecy, stored only in Azerbaijan, processed over end-to-end encrypted channels, and not subcontracted to third parties (points 2.1.9, 4.10.2.4, 4.10.2.5 and 4.10.2.8).

Deposit insurance

The Deposit Insurance Fund pays 100% of an insured deposit up to AZN 100,000 per depositor per participating bank; for accounts that individuals hold for business activity the cap is AZN 20,000 (Law on Deposit Insurance No 226-IIIQ, article 26.1). Deposits taken above the protected interest rate published by the Fund (12% in manat and 2.5% in US dollars or euros as of November 2026) are not protected (article 2.1.2.6).

Correspondent banking

Before opening a correspondent account for a foreign bank, a local bank must obtain and verify documents on the respondent, assess and report on the risks, and have the relationship approved by its competent management body (Regulations on opening, maintaining and closing bank accounts, points 8.1 and 8.3). Payable-through use requires CDD on the third parties (8.2), shell banks must be refused (8.4.4), and banks publish a register of the financial institutions they hold such relationships with (8.7).

8 Risk indicators and red flags

SELECTED BANK CRITERIA PUBLISHED BY THE FINANCIAL MONITORING SERVICE

- **Shared phone number**: accounts of different people linked to the same mobile number (criterion 21).
- **Account farming**: one individual managing accounts of five or more unrelated people, including through a mobile app (27).
- **Foreign IP use**: services used from 3 or more foreign countries' IP addresses in a day, or 10 or more in 30 days (26).
- **Pass-through accounts**: over AZN 2,000 a day received from others with 90% moved on within 24 hours (30).
- **Top-up cycling**: more than 30 incoming payments a day, mainly top-ups, with over 90% forwarded (28).
- **Card inflows**: 300 or more incoming card transfers totalling AZN 15,000 or more in a month to an individual who is not a registered taxpayer (4).
- **Crypto flows**: USD 30,000 or more a month moved for buying or selling cryptocurrency (12).
- **Shell companies**: transactions by shell-type companies (23).

The Financial Monitoring Service's typologies also describe card-data and one-time-password phishing cashed out through other people's cards, and fake cryptocurrency schemes funded by card top-ups.

9 Enforcement and penalties

AML breaches by financial institutions are administrative offences under article 598 of the Code of Administrative Offences `In force`. Fines are set per breach and, for most offences, per customer or transaction:

Breach (article 598)	Officers	Legal entity
CDD, record-keeping, reliance, internal control, PEP or new-technology requirements; ignoring Financial Monitoring Service instructions; obstructing supervisors (598.1)	AZN 2,000 to 4,000	AZN 20,000 to 30,000

Failure to report transactions to be monitored, per transaction (598.4)	AZN 2,000 to 4,000	AZN 20,000 to 30,000
Breaching the duty not to execute a suspicious transaction, per transaction (598.5)	AZN 3,000 to 5,000	AZN 30,000 to 40,000
Ignoring a suspension decision, per transaction (598.6)	AZN 4,000 to 6,000	AZN 40,000 to 50,000
Failing to freeze assets under the Targeted Financial Sanctions Law, per person (598.10)	AZN 3,000 to 5,000	AZN 30,000 to 50,000

CBAR may also apply corrective measures and dismiss bank officers (Law on Banks article 49.1). In 2025, it imposed AML fines totalling AZN 644,000 under article 598 on 3 banks, 9 non-bank credit institutions, 4 payment institutions, 3 e-money institutions, a currency exchange office, an investment company and Azerpost (CBAR report on main goals and functions in 2025).

10 Recent changes and what to watch

- **1 January 2027** `Adopted, effective 1 Jan 2027`: FMS Decision No 3-21-28/3-6-7/2026 adds monthly aggregation (AZN 50,000) to wire reporting for individuals other than sole proprietors and replaces the reporting procedure. FMS Decision No 3-21-28/3-6-17/2026 (25 September 2026) moved the start from 1 October 2026 and repealed back-filing of beneficial owner data.
- **1 January 2027** `Adopted, full compliance 1 Jan 2027`: Basel III capital structure and buffers become binding.
- **26 May 2026** `Adopted, measures 2027 to 2030`: the State Programme on expanding financial inclusion for 2027 to 2030 plans a digital identity and digital profile, a distributed electronic know-your-customer (e-KYC) system, a fintech framework, and simpler remote account opening for small businesses in 2027 to 2028.
- **30 March 2026** `In force`: CBAR's remote opening Regulation extends remote onboarding to all payment accounts and requires an enhanced electronic signature for the contract.
- **23 January 2026** `Published`: MONEYVAL's 1st Enhanced Follow-up Report, adopted on 10 November 2025, re-rated Azerbaijan on R.8, R.14, R.16 (wire transfers), R.24, R.26 (supervision), R.33 and R.34; R.15 (new technologies) remains partially compliant.

- **11 April 2025** `In force`: Law No 175-VIIQD requires beneficial owner data on corporate customers to be sent to the Financial Monitoring Service within 3 working days and adds beneficial owner data to the state register of legal entities.
- **9 April 2025** `In force`: CBAR information security requirements, including in-country storage of sensitive data in the cloud.

11 What this means for identity verification

- **Documents:** support the Azerbaijani identity card as the core document, plus foreign passports and residence permits.
- **Remote method:** plan for video (live call or recorded session) for every new remote customer.
- **Biometrics:** liveness with at least three randomised actions and an automated face match against the state photo are mandatory, so the flow depends on integration with state databases.
- **Signature and authentication:** integrate an enhanced electronic signature (CBAR names ASAN İmza and SİMA) and two-factor authentication.
- **Hosting:** banks' cloud contracts must keep sensitive customer data in Azerbaijan and bar subcontracting, so a cloud-hosted verification service needs in-country storage.
- **Eligibility:** route proxies and non-resident legal entities to branch onboarding.
- **Evidence and refresh:** keep video, audio, images and logs for at least 5 years after the relationship ends, and refresh CDD every 1, 2 or 3 years by risk tier.

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 account opening with ID document capture, randomised biometric liveness and face match, built around the Central Bank's remote opening rules.
- Video KYC with recorded sessions and audit logs for the live or recorded video that new remote customers require.
- AML screening against sanctions and PEP lists at onboarding and on an ongoing basis, plus KYB and beneficial owner verification for corporate clients.
- E-signature steps and configurable risk-based workflows, with usage limits until verification is complete.

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 No 781-VIQ (Law on the Prevention of the Legalization of Criminally Obtained Property and the Financing of Terrorism)**, 30 December 2022, as amended, e-qanun.az/framework/53369
- **Banklar haqqında Qanun No 590-IIQ (Law on Banks)**, articles 3, 6 to 8, 41, 49, e-qanun.az/framework/5825
- **Əmanətlərin sığortalanması haqqında Qanun No 226-IIIQ (Law on Deposit Insurance)**, article 26, e-qanun.az/framework/12137
- **Hədəfli maliyyə sanksiyaları haqqında Qanun No 782-VIQ (Law on Targeted Financial Sanctions)**, e-qanun.az/framework/53362

- **Fərdi məlumatlar haqqında Qanun No 998-IIIQ (Law on Personal Data)**, article 9, e-qanun.az/framework/19675
- **İnzibati Xətalar Məcəlləsi (Code of Administrative Offences)**, article 598, e-qanun.az/framework/46960
- **Law No 175-VIIQD amending the Tax Code and laws on state registration of legal entities, banks, AML and others**, 11 April 2025, articles 4, 10 and 12, Milli Məclis, meclis.gov.az
- **State Tax Service under the Ministry of Economy, Notice on beneficial owners**, taxes.gov.az
- **Presidential Decree No 361 on ensuring the implementation of the Law on Personal Data**, 13 December 2010, as amended, point 3, mincom.gov.az
- **Presidential Decree No 676 on measures to improve management in the field of cybersecurity**, 2 June 2026, and the Charter of the National Cybersecurity Agency, points 3.1.24 and 3.1.25, e-qanun.az/framework/61938
- **Financial Monitoring Service Decision No 3-21-28/3-6-4/2023, Rules on verification measures during CDD and the application of new technologies, risk factors and risk groups**, 21 February 2023, as amended 14 June 2024, e-qanun.az/framework/53641
- **Financial Monitoring Service Decision No 3-21-28/3-6-8/2023 on reporting procedure and minimum thresholds**, 27 April 2023, e-qanun.az/framework/54120
- **Financial Monitoring Service Decision No 3-21-28/3-6-7/2026 amending Decision No 3-21-28/3-6-8/2023**, 21 April 2026, effective 1 January 2027, as amended by **Financial Monitoring Service Decision No 3-21-28/3-6-17/2026** of 25 September 2026, e-qanun.az/framework/62373
- **Financial Monitoring Service, Criteria for identifying suspicious transactions and cases by banks**, and published typologies, fiu.gov.az/az/special-indicators, fiu.gov.az/az/typologies
- **CBAR Board Decision No 44/5, Regulation on remote opening of accounts**, 16 December 2025, in force 30 March 2026, e-qanun.az/framework/61120
- **CBAR Board Decision No 04/2, Regulations on opening, maintaining and closing bank accounts**, 4 February 2022, as amended, chapter 8, e-qanun.az/framework/49456
- **CBAR Board Decision No 09/1, Rules on applying CDD measures to electronic transfers of funds**, 22 February 2023, e-qanun.az/framework/53633
- **CBAR Board Decision No 12/2, Rules on application of strong customer authentication**, 13 March 2024, e-qanun.az/framework/56660
- **CBAR Board Decision No 14/2, Requirements on ensuring information security in entities supervised in financial markets**, 28 March 2024, in force 9 April 2025, e-qanun.az/framework/56708
- **CBAR Board Decision No 16/1-2, Rules on calculation of bank capital and its adequacy**, points 3.2 and 3.6, e-qanun.az/framework/44968
- **CBAR, Report on accomplishment of main goals and functions in 2025**, sections 2.6.4 and 2.7, cbar.az
- **Presidential Order No 1048 approving the State Programme on expanding financial inclusion in Azerbaijan for 2027 to 2030**, 26 May 2026, cbar.az
- **Deposit Insurance Fund**, protected deposit rates and compensation, adif.gov.az

- **MONEYVAL, Anti-money laundering and counter-terrorist financing measures, Azerbaijan, 1st Enhanced Follow-up Report & Technical Compliance Re-Rating, MONEYVAL(2025)16**, December 2025, adopted by written procedure on 10 November 2025, rm.coe.int
- **Council of Europe, Money laundering and terrorist financing progress reports on Azerbaijan, Croatia and Estonia**, 23 January 2026, coe.int