Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Azerbaijan

COUNTRY Azerbaijan

INDUSTRY Telecom & Mobile Services

LAST UPDATED 13 November 2026

KEY REGULATORS Ministry of Digital Development and Transport · Ministry of Economy · State Tax Service

Key takeaways

- Every SIM in Azerbaijan is tied to a named, identified person. Operators may switch on a mobile or fixed number only after the customer's data has been checked against state records and entered online into a single subscriber database.
- The subscriber contract must be in Azerbaijani and carry a copy of the customer's photo identity document. When a company buys the line, the identity document of the person who will actually use it is attached.
- SIM activation rules are the same online and in a shop: there is no lighter regime for eSIM (a downloadable SIM profile) or web sales, and dealers are bound too. Remote biometric identification is expressly regulated for one related service: issuing electronic signature certificates.
- Telecom operators are not covered by the anti-money laundering (AML) law, so no customer risk scoring or suspicious-transaction reporting applies. Asset-freeze duties under the sanctions law, data protection rules and device registration still do.
- Handsets are registered by their IMEI (the unique device number). Operators must cut service to blacklisted devices within 24 hours, and fines for a company reach AZN 20,000 for a repeat breach.

The market is open to licensed operators, but entry is costly and controlled: a cellular (mobile) licence is issued by the Ministry of Digital Development and Transport for ten years against a state duty of AZN 1,000,000, and it has no legal effect until a licence contract is signed within 30 days. Other telecom services are licensed by the Ministry of Economy at much lower duties.

The Ministry of Digital Development and Transport is the central authority: it supervises telecoms, issues mobile licences, runs the Data Computing Centre behind the subscriber database, sets up the device registration system and remains the personal data authority. Since 2 June 2026 its National Cybersecurity Agency keeps the state register of personal data systems and examines personal data complaints. The State Tax Service matters because a SIM or eSIM can carry the ASAN İmza mobile signature, a state-recognised digital identity.

The biggest obstacle for a new entrant, including a digital-only brand, is that onboarding must plug into state infrastructure: an identity check through the ministry's Data Computing Centre against state registers, and an online feed into the unified subscriber database before any number goes live.

CONTENTS

1 Who regulates this sector
2 Licensing and authorisation
3 Identity framework (AML rules do not apply)
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 in telecom	Level	Official site
Ministry of Digital Development and Transport	Telecom policy and supervision; cellular licences and licence contracts; licences for biometric technologies and personal data systems; Data Computing Centre (subscriber database, number portability database); Mobile Device Registration System; personal data authority. Its National Cybersecurity Agency (created on 2 June 2026 on the basis of the Electronic Security Service) regulates cybersecurity, keeps the state register of personal data systems and examines personal data complaints	National	mincom.gov.az
Ministry of Economy	Licences for fixed telephony, radio trunking, IP telephony, data transmission and telecom channels	National	economy.gov.az
Cabinet of Ministers	Subscriber data conditions for operators and dealers; Mobile Device Registration Rules; electronic signature certificate rules	National	nk.gov.az
ASAN Certification Services Center of the State Tax Service	Issues certificates for the SIM and eSIM-based ASAN İmza mobile signature	National	taxes.gov.az

Ministry of Internal Affairs	Receives and pools reports of lost or stolen SIM cards and handsets	National	mia.gov.az
Financial Monitoring Service	Receives targeted financial sanctions freeze reports; telecom operators are not AML obliged entities	National	fiu.gov.az

Courts and law enforcement bodies are not regulators, but their requests for subscriber data carry statutory response deadlines (section 7).

2 Licensing and authorisation

Article 8 of the **Law on Telecommunications No 927-IIQ** leaves licensing to the **Law on Licences and Permits No 176-VQ of 15 March 2016**. Fixed and data services sit in its annex 1; cellular services, biometric technologies and personal data systems sit in annex 2, the list of activities licensed for state-security reasons. Presidential Decree No 866 of 20 April 2016 makes the Ministry of Economy the licensing authority for annex 1 and the Ministry of Digital Development and Transport for annex 2 items 3, 4 and 4-1 (paragraphs 2.3.1, 2.3.4). Duties are set by article 22 of the **Law on State Duty**:

Activity	Issuing authority	State duty	Term
Cellular (mobile) services, by technology standard	Ministry of Digital Development and Transport	AZN 1,000,000	10 years
IP telephony	Ministry of Economy	AZN 50,000	Indefinite
International telecom channels	Ministry of Economy	AZN 5,500	Indefinite
Data transmission	Ministry of Economy	AZN 3,000	Indefinite
Fixed telephony; radio trunking and wireless telephony; domestic channels	Ministry of Economy	AZN 2,500 each	Indefinite
Creating and servicing biometric technologies	Ministry of Digital Development and Transport	AZN 1,100	Indefinite

Personal data information resources and systems	Ministry of Digital Development and Transport	AZN 1,100	Indefinite

The licensing authority decides within 10 working days of registering an application (article 19.8). A cellular licence is followed within 30 days by a licence contract with the ministry, without which the licence has no legal effect (article 19.8-1). The contract form, approved by the ministry's collegium on 7 September 2020, carries the operator's subscriber identification, number portability and device-blocking duties. Radio frequencies are assigned separately and fall away when the service licence is revoked or a cellular licence expires (Telecommunications Law, article 13).

Internet service operators and providers must register with the ministry within 15 days of starting service (article 13-1; registration rules approved by Cabinet Decision No 427 of 12 October 2017). Neither licence annex has a separate category for mobile virtual network operators, so a reseller model must be built around an existing licence; most operator duties in article 33 extend to providers (article 33.2).

3 Identity framework (AML rules do not apply)

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, lists its obliged entities in articles 1.1.7 to 1.1.9: credit organisations, life insurers, investment firms, payment and e-money institutions, virtual asset service providers, the national postal operator, and designated non-financial businesses such as casinos, realtors and notaries. Telecom operators are not on the list, so they have no statutory duty to risk-rate customers, verify beneficial owners or file suspicious transaction reports. An operator that also runs a payment or e-money business falls within article 1.1.8 for that business.

Identity in telecoms is instead governed by three layers:

Telecommunications Law

Article 40.3-1: contract in Azerbaijani with a copy of the subscriber's photo identity document. Article 33.1.3-3: numbers activated only after the applicant's data is entered online into the unified database.

Cabinet conditions

Cabinet Decision No 131 of 7 July 2005, last amended on 27 October 2026, sets the identification route and, in its 2015 conditions, the data fields.

Device registration

Article 25 of the Telecommunications Law and the Mobile Device Registration Rules (Cabinet Decision No 212 of 28 December 2011, as amended) bind each handset's IMEI to the network.

Sanctions apply to everyone. Under article 5.1 of the **Law on Targeted Financial Sanctions No 782-VIQ**, all natural and legal persons in Azerbaijan must freeze designated persons' assets without delay and without notice once a listing is published on the sanctions information resource, and report immediately through it. Telecom operators are covered as legal persons in Azerbaijan.

Records: article 48.5 of the Telecommunications Law requires mobile operators to keep all registered data on foreign roaming users for at least one year.

4 Identity verification and onboarding

Accepted documents

The annex to the conditions names the documents from which the subscriber's details are taken: the identity card or general passport of an Azerbaijani citizen, the document of a stateless person or foreigner permanently resident in Azerbaijan, the refugee card of a recognised refugee, or a foreign citizen's passport. The contract carries a copy of a photo identity document; for a corporate subscriber, the identity document of the natural person who uses the line.

Data captured

For an individual: full name, document name, number and issue date, personal identification number (FİN), citizenship, place and date of birth, and full residential address down to flat number. For a legal entity: name, country of registration, tax identification number (VÖEN), bank details and the authorised representative's name and document number. Contract and database both hold the phone number, SIM number, activation date and dealer or distributor; the database adds the IMSI, the handset's IMEI, dealer and distributor codes and the identity document number of the employee who accepted the contract. All data is recorded in Azerbaijani, in Unicode.

Verification against state records

Under paragraph 2.1 of Decision No 131, applicant data is identified through the Data Computing Centre of the Ministry of Digital Development and Transport: for individuals against the interagency Entry-Exit and Registration system, and for legal entities, since 28 October 2026, through state information systems and resources integrated into the Electronic Government Information System. Once the data is entered online into the unified database of the operators and the Data Computing Centre, the number is activated within 24 hours. The check is documentary verification against state registers; the conditions do not require selfie matching, liveness detection or chip reading.

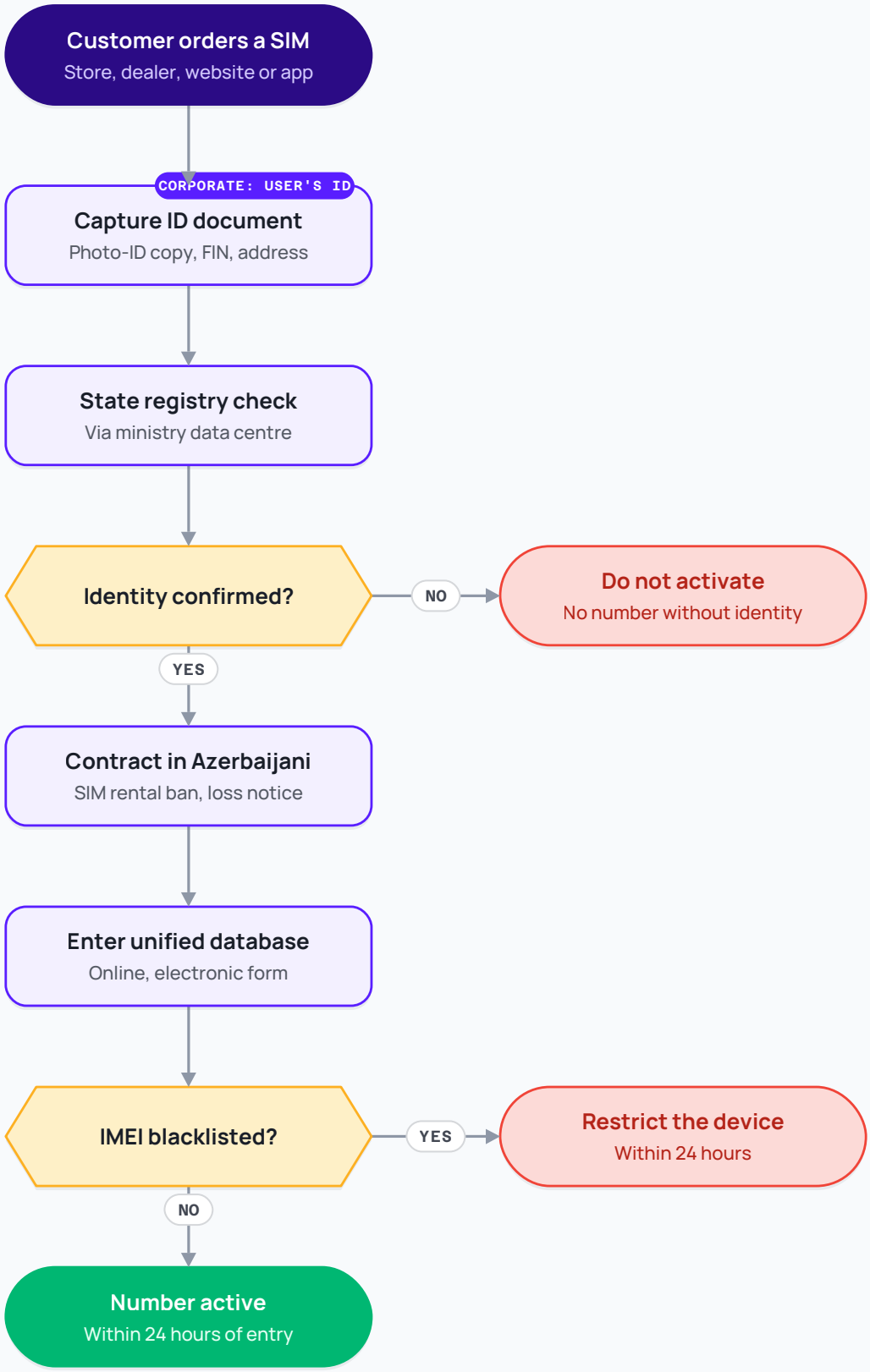


Figure 1. SIM and eSIM activation for a new subscriber in Azerbaijan.

The SIM as an identity credential

ASAN İmza, operated by the State Tax Service with the mobile operators, binds signature certificates to a SIM; the State Tax Service describes it as mobile identification with the same legal force as a handwritten signature. As of July 2025 the State Tax Service directs applicants to buy an ASAN İmza SIM from a mobile operator and bring it, with an identity document, to a State Tax Service centre, an SME house or an ASAN Service centre; its procedure page gives one working day for the certificate. An eSIM-based version has been offered since December 2023. The alternative SİMA İmza, which the Ministry of Digital Development and Transport describes as a cloud signature using face recognition, is obtained by registering in a smartphone app.

5 Digital channels: what's different

Bottom line: SIM activation is channel-neutral. A number sold online or as an eSIM needs the same photo-ID copy, state-registry check and database entry as one sold in a shop; the explicit remote rules sit in signature certificates (biometric identification and video) and device registration (e-government identification).

Requirement	In person / store	Online / remote	Difference
Contract with photo-ID copy	Required (art. 40.3-1)	Required; no remote exception	Same
Data fields	Full list in the conditions	Same list	Same
Identity check	Data Computing Centre against state registers	Same route	Same
When the number goes live	After online database entry, within 24 hours	Same	Same
Who is bound	Operators, dealers, distributors	Same	Same
Device registration	Registration centre, operator service desk or post office	Online after identification in the e-government system	Differs

Consent to data processing	Written consent	Electronic document with enhanced e-signature, or via the e-government system	Differs
Signature certificate	ASAN İmza: SIM and identity document presented at a service centre	Rules allow biometric identification, with biometric data and video kept; SİMA İmza is registered in an app	Differs

No separate eSIM or remote activation regime

Neither the Telecommunications Law nor Decision No 131 distinguishes between sales channels. A digital sales flow must therefore capture an image of the identity document for the contract and route the data through the same state check.

Remote identification for signature certificates

Cabinet Decision No 461 of 22 October 2024 amended the Rules on providing certification services (Cabinet Decision No 27 of 2006). When an accredited certification centre serves an applicant remotely, it must confirm identity by biometric identification and handle the application, disclosures and contract through its own software (paragraph 3.1-1). The lookup records, biometric data and video of the application are stored in the centre's database (paragraph 3.1-2). In practice, a first ASAN İmza certificate is still issued at a service centre and existing certificates can be renewed online, while SİMA İmza registration runs in a smartphone app.

Electronic consent

Article 8.1 of the **Law on Personal Data No 998-IIIQ** accepts written consent as an electronic document with an enhanced electronic signature, and article 8.2 allows consent through the Electronic Government Information System. Article 8.4 puts the burden of proving consent on the data owner or operator, so a remote flow should keep the signed record.

6 Data protection and biometrics

The Law on Personal Data No 998-IIIQ is the general regime. Article 9.5 applies its full conditions to biometric data, naming fingerprints and palm prints, facial images, iris and retina, voice samples, DNA results, handwriting and signatures. An operator that adds face matching to remote activation processes biometric data under the same consent and

security rules, and anyone who creates or services biometric technologies needs a licence from the Ministry of Digital Development and Transport.

Article 15 requires personal data information systems to be registered with the state before data is collected; processing in an unregistered system is prohibited. The Ministry of Digital Development and Transport remains the personal data authority under Presidential Decree No 361 of 13 December 2010. Since 2 June 2026, its National Cybersecurity Agency, created by Presidential Decree No 676 on the basis of the Electronic Security Service, keeps the state register of personal data systems and examines complaints from data subjects (Charter, paragraphs 3.1.24 and 3.1.25). Article 9.4 requires data to be destroyed without delay once its purpose is achieved.

Article 14 prohibits cross-border transfer where it threatens national security or the destination does not protect data to the Azerbaijani level, unless the subject consents. Article 38 of the Telecommunications Law adds confidentiality of communications: data on network use may be disclosed only in cases set by law.

7 Sector-specific obligations

Mandatory contract clauses

Article 40.3 of the Telecommunications Law requires every subscriber contract to state that the SIM may not be handed to others for permanent use or rented out for regular income (40.3.5-2), that loss or theft of the SIM or handset must be reported immediately (40.3.5-3; the conditions name local bodies of the Ministry of Internal Affairs, which pools the reports), and whether the subscriber consents to appearing in directories (40.3.9).

Mobile device registration

Article 25, added by Law No 771-VIQ of 27 December 2022, requires mobile devices to be registered and prohibits altering or cloning an IMEI. Under the Mobile Device Registration Rules, the ministry sets up the Mobile Device Registration System and supervises its registration centre. Operators restrict blacklisted devices within 24 hours, except IMEIs matched to a specific number on the whitelist, and tell the subscriber by SMS when a device in use is blacklisted after a cloning check. A device brought in for personal use must be registered within 30 days; the state duty runs from AZN 15 to AZN 100 by market price, and AZN 100 for each further device in a calendar year (Law on State Duty, article 33-5); roaming visitors are exempt. Cabinet Decision No 191 of 12 June 2023 lets the registration centre obtain MSISDN, IMSI and call detail records from operators online to trace cloned devices.

Number portability and paid services

Under the cellular licence contract, operators connect to the central number portability database run with the Data Computing Centre and must prevent unjustified refusals of port requests, including from corporate customers (clauses 6.6.6 and 6.6.7). Subscribing a customer to paid value-added services requires two-step confirmation of consent (clause 6.7.7.4).

Disclosure, blocking and incident reporting

Operators answer requests from the relevant executive authority, courts and law enforcement within three working days, or immediately (at most 24 hours) when marked urgent (article 33.1.9-2), equip networks for lawful interception (article 39), block illegal gambling including foreign betting operators (article 33.1.9-6), and act against illegal international traffic (article 33.1.9-3). Since 10 August 2026, the Law on Information requires owners of information infrastructure, including internet providers, to report cyber incidents to the National CERT immediately on detection.

8 Risk indicators and red flags

TELECOM IDENTITY-ABUSE INDICATORS DRAWN FROM AZERBAIJANI RULES

- **SIM rental**: one subscriber's SIMs used by others for regular income, a fineable offence.
- **Unregistered activation**: a dealer activates numbers before the data reaches the unified database.
- **Corporate lines without a named user**: company SIMs with no user's photo-ID copy attached.
- **IMEI cloning**: one IMEI seen on several devices or subscribers.
- **Blacklisted handsets**: attempts to connect devices on the registration blacklist.
- **Bypass traffic**: international calls terminated through local SIMs or equipment outside licensed routes.
- **Lost or stolen SIMs**: activity after the subscriber reports loss or theft.

9 Enforcement and penalties

Penalties sit in the **Code of Administrative Offences** and are fixed amounts or ranges per offence, with higher amounts for a repeat within one year of the first penalty decision taking effect.

Offence (article)	Officials	Legal entities	Repeat within a year
Required data missing from contracts or subscriber databases (362-1)	AZN 2,000	AZN 3,000	AZN 4,000 / 6,000
Activating a number without online database entry (362-2)	AZN 2,000	AZN 3,000	AZN 4,000 / 6,000
Renting out a SIM or handset for regular income (368); individuals AZN 300 to 500	AZN 1,000 to 2,000	AZN 3,000 to 5,000	Not specified
Altering or cloning an IMEI (368-1); individuals AZN 300 to 400	AZN 1,000 to 1,500	AZN 3,000 to 4,000	AZN 2,000 to 2,500 / 9,000 to 12,000
Serving a blacklisted device (369)	AZN 1,000 to 2,000	AZN 8,000 to 10,000	AZN 3,000 to 4,000 / 16,000 to 20,000
Personal data breaches, incl. unregistered systems (375)	AZN 300 to 500		Not specified

Article 39.2 of the Telecommunications Law adds liability for failing to support lawful interception, and for activities licensed under annex 1 of the Law on Licences and Permits, a supervising body that finds breaches or unheeded instructions sends the licensing authority a reasoned submission to suspend or revoke the licence (article 27.3).

10 Recent changes and what to watch

- **27 October 2026** `In force from 28 Oct 2026` Cabinet Decision No 361 routes legal-entity subscriber checks through systems integrated into the Electronic Government Information System and moves online device registration to e-government identification.

- **10 August 2026** `In force` Law No 454-VIIQD adds a cybersecurity chapter to the Law on Information: immediate incident reporting to the National CERT and 24-hour answers to its requests.
- **30 June 2026** `Adopted, applies from 5 Aug 2027` Law No 431-VIIQD bars under-16s from listed social network platforms and requires age checks using bank card, email and mobile number data, adding lookups that rely on subscriber identity.
- **2 June 2026** `In force` Presidential Decree No 676 creates the National Cybersecurity Agency under the Ministry of Digital Development and Transport, which now keeps the personal data systems register and handles personal data complaints.
- **22 October 2024** `In force` Cabinet Decision No 461 allows certification centres to issue signature certificates remotely with biometric identification and stored video.
- **12 June 2023** `In force` Cabinet Decision No 191 prohibits service to blacklisted IMEIs and gives the registration centre online access to operators' MSISDN, IMSI and call records.
- **27 December 2022** `In force` Law No 771-VIQ puts mobile device registration and the IMEI rules into the Telecommunications Law itself.

11 What this means for identity verification

- **Documents:** support Azerbaijani identity cards and passports, residence documents, refugee cards and foreign passports; capture an image good enough to serve as the contract copy.
- **Data, not just images:** extract every field in the annex to the conditions, including FİN and full address, and record it in Azerbaijani in Unicode.
- **State check first:** the authoritative check is the registry lookup through the Data Computing Centre; biometric steps are optional for SIM sales but mandatory for remote signature certificates, where video must also be kept.
- **Corporate lines:** capture the end user's identity document as well as the company's VÖEN and representative.
- **Device binding:** collect the IMEI at activation and act on blacklist changes within 24 hours.
- **Consent and records:** keep enhanced e-signature or e-government consent records, and register the information system that stores onboarding data before going live.

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:

- ID document capture and verification for Azerbaijani identity cards, passports and foreign documents, with the image retained for the subscriber contract.
- Data extraction for every required subscriber field, ready to feed the operator's activation and database workflow.
- Optional face match and biometric liveness for remote SIM and eSIM sales, configured in a no-code workflow builder.
- Phone and email verification and e-signature steps for online contracts and consent records.
- Cloud, on-premises or hybrid deployment to fit local data and information-system registration requirements.

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

- **Telekommunikasiya haqqında Qanun No 927-IIQ [Law on Telecommunications]**, consolidated text to Law No 488-VIIQD of 13 October 2026, articles 8, 13, 13-1, 25, 33, 38, 39, 40, 48, e-qanun.az/framework/10663
- **Law No 771-VIQ of 27 December 2022 amending the Law on Telecommunications** (article 25), Milli Məclis, meclis.gov.az
- **Cabinet of Ministers Decision No 131 of 7 July 2005** with the Conditions approved by Decision No 200 of 22 May 2015 and annex, consolidated to Decision No 361 of 27 October 2026, e-qanun.az/framework/10541

- **Cabinet of Ministers Decision No 361 of 27 October 2026** (paragraphs 2 and 4), e-qanun.az/framework/62848
- **Mobile Device Registration Rules, Cabinet of Ministers Decision No 212 of 28 December 2011**, consolidated, paragraphs 1.4, 2, 3, 4.4, 5, e-qanun.az/framework/22857
- **Cabinet of Ministers Decision No 191 of 12 June 2023 amending the Mobile Device Registration Rules**, nk.gov.az PDF
- **Presidential Decree No 866 of 20 April 2016 on applying the Law on Licences and Permits**, paragraphs 2.3.1 and 2.3.4, e-qanun.az/framework/32627
- **Lisenziyalar və icazələr haqqında Qanun No 176-VQ [Law on Licences and Permits]**, articles 19.8, 19.8-1, 22.1, 22.1-1, 27.3, annexes 1 and 2, e-qanun.az/framework/32626
- **Dövlət rüsumu haqqında Qanun No 223-IIQ [Law on State Duty]**, articles 22.0.6, 22.0.37, 22.0.38, 33-5, e-qanun.az/framework/2860
- **Licence contract form and conclusion rules**, Ministry of Digital Development and Transport collegium decision KQ-6/20 of 7 September 2020, clauses 6.6.4, 6.6.6, 6.6.7, 6.7.7.4, e-qanun.az/framework/45992
- **Law on the Prevention of the Legalization of Criminally Obtained Property and the Financing of Terrorism (AML/CFT Law), No 781-VIQ of 30 December 2022**, official English title per the Financial Monitoring Service, articles 1.1.7 to 1.1.9, e-qanun.az/framework/53369
- **Hədəfli maliyyə sanksiyaları haqqında Qanun No 782-VIQ [Law on Targeted Financial Sanctions]**, official English title per the Financial Monitoring Service, article 5.1, e-qanun.az/framework/53362
- **Fərdi məlumatlar haqqında Qanun No 998-IIIQ [Law on Personal Data]**, articles 8, 9, 14, 15, e-qanun.az/framework/19675
- **Presidential Decree No 676 of 2 June 2026 on improving cybersecurity governance**, with the Statute of the National Cybersecurity Agency, paragraphs 1 and 3, and Charter paragraphs 3.1.24-3.1.25, e-qanun.az/framework/61938
- **Presidential Decree No 361 of 13 December 2010 on ensuring implementation of the Law on Personal Data**, paragraph 3.1, e-qanun.az/framework/21035
- **Cabinet of Ministers Decision No 461 of 22 October 2024 amending the Rules on providing certification services**, paragraphs 3.1-1 to 3.1-3, e-qanun.az/framework/58176
- **Law No 454-VIIQD of 14 July 2026 amending the Law on Information, Informatisation and Protection of Information**, articles 20-7 to 20-11, e-qanun.az/framework/62415
- **Law No 431-VIIQD of 30 June 2026** (social network age limits), mincom.gov.az, mincom.gov.az PDF
- **Frequently asked questions (SİMA)**, Ministry of Digital Development and Transport, mincom.gov.az
- **Cabinet of Ministers Decision No 427 of 12 October 2017 approving the rules for registering internet service operators and providers**, mincom.gov.az, mincom.gov.az PDF
- **İnzibati Xətalar Məcəlləsi [Code of Administrative Offences]**, articles 362-1, 362-2, 368, 368-1, 369, 375, e-qanun.az/framework/46960

- **Measures to protect personal data more reliably**, State Tax Service, 4 July 2025, taxes.gov.az; **ASAN İmza**, State Tax Service, taxes.gov.az; **New generation digital ASAN İmza service**, 28 December 2023, taxes.gov.az