Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Azerbaijan

COUNTRY Azerbaijan

INDUSTRY Government & Public Services

LAST UPDATED 14 November 2026

KEY REGULATORS Ministry of Digital Development and Transport · Innovation and Digital Development Agency

Key takeaways

- Public bodies in Azerbaijan must log users into their online services through the EGIS single sign-on (Vahid Giriş), operated as mygov ID. Users choose from a short list of state-recognised login methods.
- Identity card data pulled from the national Electronic Government Information System (EGIS) counts legally as showing the physical card, so online services can rely on it instead of document uploads.
- Only an "enhanced" electronic signature backed by an advanced certificate carries the same legal weight as a handwritten signature. Foreign non-residents can obtain one through Azerbaijani embassies and consulates.
- Companies that create or service biometric technology, or build and service personal data systems, in Azerbaijan need a licence from the Ministry of Digital Development and Transport.
- Anti-money laundering (AML) rules do not apply to government bodies. Identity is governed instead by the identity card, electronic signature, personal data and e-government rules, plus a Law on Public Services in force since December 2025.

Azerbaijan's public sector is a mature digital-first market: public e-services run on a central state platform, and the same identity layer is open to private relying parties through integration. Authorisation attaches to each information system and e-service, through technical, security and registration conditions set by the state, and to licensed activities such as biometric technology.

The Ministry of Digital Development and Transport owns EGIS, regulates electronic signatures and personal data systems, and licenses biometric technology. Its Innovation and Digital Development Agency (IDDA) operates EGIS, mygov and mygov ID. The biggest obstacle for a new entrant is integration: an e-service or data feed goes live only after state opinions on expediency and information security, entry in the unified register and connection to EGIS.

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	Level	Official site
Ministry of Digital Development and Transport	Owner of EGIS; competent authority for electronic signatures, including accreditation of certificate centres; competent personal data authority; licenses biometric technology and personal data systems. Its National Cybersecurity Agency (Presidential Decree No 676 of 2 June 2026, created on the basis of the former Electronic Security Service) keeps the personal data system register, hears complaints and acts on violations	National	mincom.gov.az
Innovation and Digital Development Agency (IDDA)	Operator of EGIS and most subsystems, including the EGIS single sign-on (Vahid Giriş), operated as mygov ID, and the mygov platform	National (agency under the Ministry)	idda.az
Ministry of Internal Affairs	Issues identity cards and loads chip data; its local offices issue signature certificates during card personalisation	National	asan.gov.az (service page)
State Tax Service under the Ministry of Economy	Its ASAN Certification Services Center issues ASAN İmza mobile signature certificates	National	taxes.gov.az

Service providers (public bodies)	Design, register and deliver each public service under the Law on Public Services	National and local	my.gov.az (service catalogue)

2 Licensing and authorisation

Launching a public e-service

Under Article 14-1 of the Law on Information, Informatisation and Protection of Information (added by Law No 1193-VIQD of 28 June 2024, in force 16 July 2024), a public body may deliver an electronic service only after a positive opinion on the project's technical expediency (or changes made in line with it), a positive information-security opinion, entry in the unified register of state information resources, systems and e-services, and integration into EGIS. Systems delivering e-services must be monitored against security criteria, use protected channels and pass a security audit at least once a year (Article 14). The Law on Public Services (No 279-VIIQ of 31 October 2025, in force 3 December 2025) adds that, from 1 January 2026, no public service may be provided until it is entered in the Electronic Register of Public Services (Article 6.4).

Licences for identity technology suppliers

Annex 2 of the Law on Licences and Permits (No 176-VQ of 15 March 2016) lists activities licensed for reasons of state security. Two of them cover identity vendors: creating and servicing biometric technologies, and forming personal data information resources and creating and servicing information systems for them. The Ministry of Digital Development and Transport issues both licences, each for a state duty of AZN 1,100. This mirrors Article 5.1 of the Law on Biometric Information (No 651-IIIQ of 13 June 2008).

Certificate service providers

Under the Law on Electronic Signature and Electronic Document (No 602-IIQ of 9 March 2004), only a centre accredited by the competent authority, the Ministry of Digital Development and Transport, may issue the advanced ("təkmil") certificates behind legally equivalent signatures (Articles 1.1.14 and 11.3; Presidential Decree No 65 of 26 May 2004, paragraph 2.3).

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) applies to financial institutions and to listed non-financial businesses and professions: casino organisers and operators, and realtors, lawyers, notaries and independent legal, accounting and tax advisers when they carry out specified transactions (Articles 1.1.7 to 1.1.9 and 3.1). Ministries, agencies and municipalities delivering public services are not obliged entities, so the AML/CFT Law imposes no customer due diligence or reporting duty on public services as such.

Identity in this sector is governed by four instruments instead:

Identity Card Law

The Law on the Identity Card of a Citizen of the Republic of Azerbaijan (1994, as amended) defines the card, its chip and the legal effect of its data when obtained through EGIS.

E-signature Law

Law No 602-IIQ sets which electronic signatures are equal to a handwritten one and how certificates are issued.

E-government rules

Presidential Decree No 472 of 12 August 2025 (the EGIS Regulation) and Cabinet Decision No 241 of 4 August 2025 (Rules on organising and providing e-services) make the single sign-on mandatory.

Personal Data Law

Law No 998-IIIQ of 11 May 2010 governs consent, biometric data, registration of data systems and cross-border transfer.

4 Identity verification and onboarding

The identity card and its chip

The Ministry of Internal Affairs issues the citizen's identity card, valid for 10 years (without limit from age 55). Its chip holds the holder's name, personal identification number (FİN), issue date, signature, an International Civil Aviation Organization (ICAO) compliant photograph and fingerprints (Identity Card Law, Article 3). Since the 2024 amendment, providing identity card data through EGIS is equal to presenting the card. Advanced

signature certificates can also be issued during personalisation of the card (E-signature Law, Articles 11.1 and 11.3-1).

Single sign-on is mandatory for public e-services

Cabinet Decision No 241 requires that users and the provider's staff are identified through the EGIS "Vahid Giriş" (single sign-on) subsystem (paragraph 2.11), which identifies users by enhanced electronic signature with an advanced certificate and other electronic identification means (EGIS Regulation, paragraph 3.14). In practice this is mygov ID: login by mygov app QR code, SİMA İmza, ASAN İmza, SİMA Token, personal identification number with password, a BSXM electronic signature or, for foreign citizens, a visitor account opened with an email address and password. Users can turn on two-factor authentication.

How users obtain credentials

ASAN İmza is a mobile signature on a SIM or eSIM, with advanced certificates from the ASAN Certification Services Center of the State Tax Service. A first-time user applies in person with an identity card at a mobile operator and activates the certificates at that centre; renewals and extra certificates can be requested online. SİMA İmza is an enhanced signature based on cloud, public-key and face recognition technology: since March 2024 the State Tax Service has applied biometric checks (face recognition, liveness test and rotation test) when SİMA is used to log in and to sign company registration documents. A mygov ID account can be opened remotely by video registration, reviewed by an operator within one working day, or immediately with SİMA İmza.

Non-residents

Under Presidential Decree No 1598 of 12 September 2017, foreigners and Azerbaijani citizens living abroad can apply online for an ASAN İmza or token-based signature certificate. If the Ministry of Internal Affairs, Ministry of Foreign Affairs, State Security Service and Foreign Intelligence Service raise no objection within three working days, the applicant receives a "virtual FİN". The applicant then attends the embassy or consulate in person with original documents and a biometric-standard photograph.

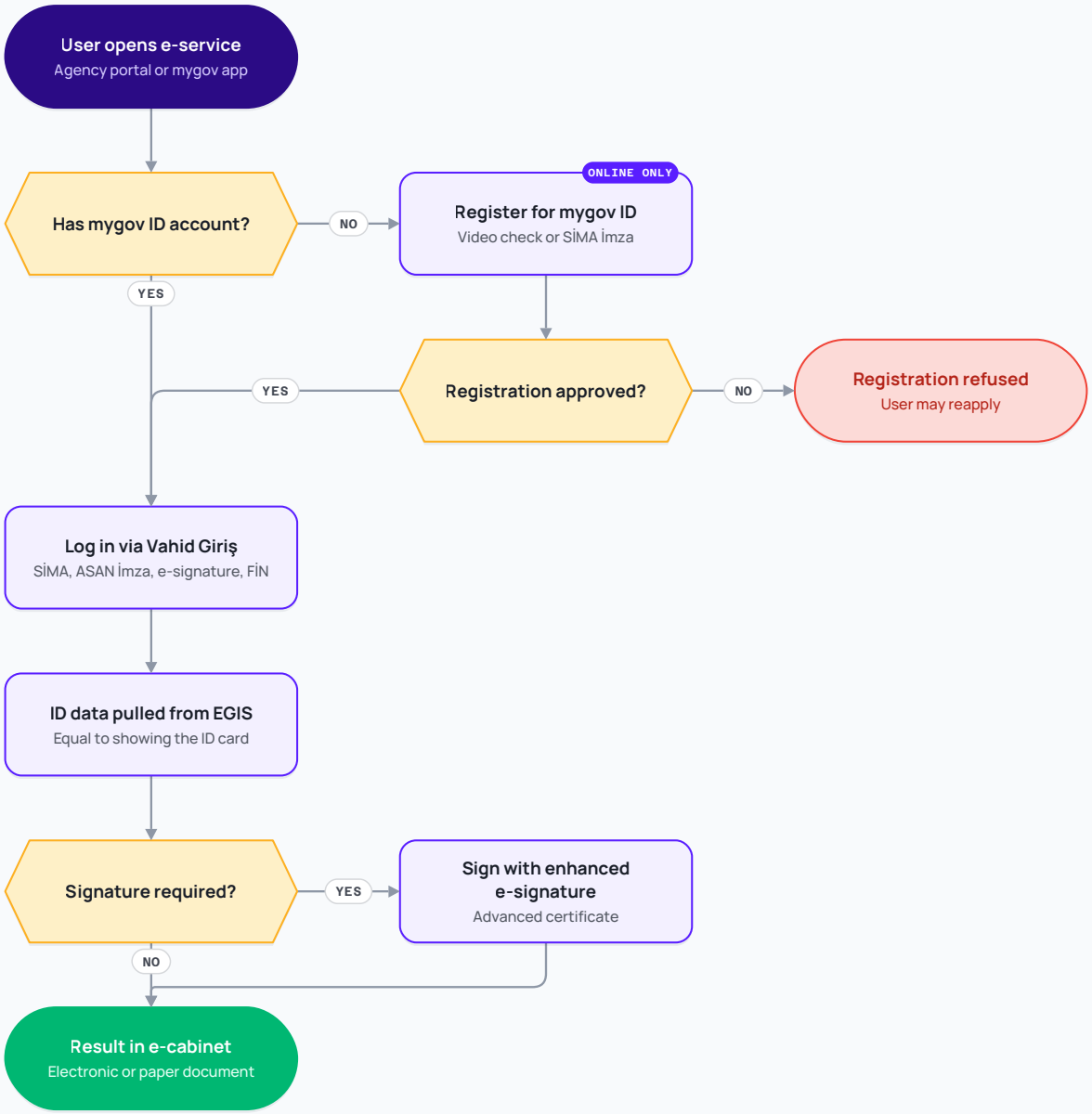


Figure 1. Remote access to a public e-service in Azerbaijan through mygov ID.

A service user may also require the provider to obtain any document available from another public body through EGIS rather than submitting it (Law on Public Services, Article 4.1.5).

5 Digital channels: what's different

Bottom line: the legal effect of identity evidence and signatures is the same online and in person, but online access must run through the state single sign-on, and the systems behind it must clear state security and registration checks before going live.

Requirement	In person	Online / remote	Difference
Legal effect of ID evidence	Physical identity card shown	ID card data obtained through EGIS, equal to showing the card	Same
Where and how access happens	Service point, call centre or mobile service	Only after identification through the Vahid Giriş single sign-on	Differs
Signature	Handwritten	Enhanced e-signature with advanced certificate, equal to handwritten	Same
ASAN İmza signature credential	SIM and certificates first issued in person with ID card	Renewal and extra certificates online; first issue not online	Differs
Account registration	No online account needed	mygov ID by operator-reviewed video (up to one working day) or SİMA İmza	Differs
Non-resident applicants	Attend an embassy or consulate with originals	Online application and security vetting first; final step still in person	Differs
System go-live conditions	Service entered in the Electronic Register of Public Services	Also security opinion, annual security audit and EGIS integration	Differs
Form of the result	Electronic document or paper act	Electronic document or paper act	Same

One door for every e-service

Identification for public e-services runs through Vahid Giriş. E-services are delivered through EGIS or an official website or sector portal that links to EGIS (Law on Public Services, Article 13.3; Law on Information, Article 14-1.2, as amended by Law No 494-VIIQD of 16 October 2026), and every user has an electronic cabinet showing the services received and the data requested about them (Article 13.4).

Assurance varies by login method

Each integrated service sets the assurance level it requires, and the single sign-on may automatically reject a login made with a method below that level; users can reach services only as far as their login method allows (mygov and mygov ID Unified Terms of Use, paragraph 3.2 and Annex No 02, paragraph 2.1). ASAN İmza rests on in-person checks and SİMA on face recognition with liveness testing, while the foreign visitor account rests on an email address and password. Whether that is enough is set service by service: the State Migration Service's portal for highly qualified migrants, for example, accepts email or other electronic identification for foreigners (Cabinet Decision No 323 of 30 October 2025, paragraph 1.7.4).

6 Data protection and biometrics

- **Biometrics.** The Personal Data Law's conditions apply in full to biometric data: fingerprints and palm prints, facial images, iris and retina, voice, DNA results, body measurements, handwriting and signatures (Article 9.5). Processing needs consent, a legal basis that defines purpose and method, anonymised research use or protection of life and health (Article 9.6).
- **Centralised consent.** Outside mandatory processing set by law, consent to collection and processing, and its withdrawal, is handled centrally through EGIS (Article 8.6, added in 2024). The mygov ID profile shows which data have been shared and lets users revoke permissions.
- **Registration and complaints.** Personal data information systems must be registered (Article 15.1), and data subjects may complain (Article 7.4), with the Ministry of Digital Development and Transport as competent authority (Presidential Decree No 361 of 13 December 2010, paragraph 3.1). Since June 2026 both sit with its National Cybersecurity Agency (Charter approved by Presidential Decree No 676, paragraphs 3.1.24 and 3.1.25).
- **Retention and transfer.** Data must be destroyed without delay once the purpose is achieved (Article 9.4). Cross-border transfer is prohibited where it threatens national security, or where the destination does not protect the data to the Azerbaijani

standard; the second bar does not apply if the person consents or the transfer protects life and health (Article 14).

The state platform sets a reference practice: under the mygov and mygov ID privacy policy, IDDA as operator records only the result of on-device fingerprint or face checks, raw biometric images are not stored or archived, and biometric templates are deleted without delay once the legal basis lapses.

7 Sector-specific obligations

Digital Consent: state data for private relying parties

The EGIS Regulation's "Digital Consent" (Rəqəmsal Razılıq) subsystem lets businesses providing digital services obtain data in real time from the primary source, including identity document data, criminal records, income and workplace data, family members, civil status acts, property, licences, notarial powers of attorney and decisions imposing fines or financial sanctions (paragraph 4.3). Company register data are available except founders, their shares and, since Presidential Decree No 620 of 13 March 2026, beneficial owners (paragraph 4.3.10). The business must obtain the person's consent and integrate with EGIS; requests without consent are refused, data are available only for the consented period and may not be passed to third parties except where law provides (paragraphs 3.5 to 3.7). Fees are agreed with the subsystem owner and the data source and may not exceed the cost of preparing and providing the information (paragraph 3.8; Law on Access to Information, Article 26.3).

Electronic Register of Public Services

Providers must submit a service's regulation to the register within 30 working days of the act creating the service, confirmed by enhanced e-signature with an advanced certificate (Law on Public Services, Articles 8.3 and 8.4).

8 Risk indicators and red flags

IDENTITY ABUSE INDICATORS FOR PUBLIC E-SERVICES

- **Look-alike domains**: sites imitating the gov.az zone, where most official state sites sit; Law No 454-VIIQD tasks the State CERT (GOV CERT) with detecting such fake domains.
- **Unsolicited signature prompts**: an ASAN İmza request whose verification code does not match the code on screen.
- **Lost or stolen SIM**: the ASAN İmza service names theft or loss of the physical SIM as a risk, which its eSIM version removes.
- **Recovery through a third-party number**: mygov ID contact numbers need not be in the user's name, so a reset code can reach someone else's phone.
- **Low-assurance accounts on high-value services**: email-and-password visitor accounts used for actions with legal consequences.
- **Onward sharing of state data**: a business passing Digital Consent data to a third party.
- **Unregistered or unlicensed systems**: personal or biometric data processed in a system not registered or by an unlicensed supplier.

9 Enforcement and penalties

Article 375 of the Code of Administrative Offences fines anyone who processes personal data in an information system that should be registered but is not, fails to protect personal data, or fails to destroy data or stop processing when the Personal Data Law requires. The fine is AZN 300 to 500, with no separate tier for legal persons. The Unified Court Portal (courts.gov.az) publishes 53 anonymised district court decisions under it between 2022 and June 2026, 41 of which imposed a penalty, most for processing data in an unregistered system (Article 375.0.1). In May 2026 the Electronic Security Service said it would act on unregistered systems and security failures, starting with telecoms; its successor, the National Cybersecurity Agency, now acts on such offences (Charter, paragraph 3.1.26).

For public bodies the main sanction is operational: an e-service may not run without a positive information-security opinion, and the designated body can issue binding instructions to remedy breaches of technical requirements (Law on Information, Articles 14 and 14-2.4). From 5 August 2027, social platforms that fail to apply the required age checks

face fines of AZN 35,000 to 40,000 for legal persons (Code of Administrative Offences, Article 388-4.3).

10 Recent changes and what to watch

- **27 October 2026**: `In force 28 Oct 2026` Cabinet Decision No 361 replaces references to the former "ASAN login" and e-government portal with EGIS and Vahid Giriş in a series of Cabinet acts.
- **16 October 2026**: `In force 28 Oct 2026` Law No 494-VIIQD aligns the Law on Information and related laws with the Law on Public Services.
- **30 June 2026**: `Adopted, applies from 5 Aug 2027` Law No 431-VIIQD bars under-16s from listed social platforms and prescribes age checks by bank card, email and mobile number, with other methods only with state approval.
- **2 June 2026**: `In force` Presidential Decree No 676 replaces the Electronic Security Service with a National Cybersecurity Agency under the Ministry, which now runs the personal data register, complaints and enforcement.
- **26 May 2026**: `Policy programme, rules not yet drafted` the State Programme on financial inclusion for 2027 to 2030 (Presidential Order No 1048) calls for a legal framework for digital identification, a distributed KYC system and e-signatures.
- **13 March 2026**: `In force` Presidential Decree No 620 removes beneficial ownership data from what private businesses can obtain through Digital Consent.
- **3 December 2025**: `In force` the Law on Public Services sets service users' rights and the rules for electronic delivery; registration before delivery applies from 1 January 2026.

11 What this means for identity verification

- **Build on the state layer.** For public e-services, user identification must come from Vahid Giriş; a separate document-and-selfie flow cannot replace it.
- **Pull, do not upload.** Identity card data from EGIS has the legal effect of the card itself. Private relying parties can obtain state-held data in real time through Digital Consent integration, with the person's consent.
- **Match the method to the action.** Use an enhanced signature with an advanced certificate where a handwritten signature would be needed; set the assurance level each service needs, since the single sign-on rejects weaker logins.

- **License before you build.** Creating or servicing biometric technology, and building personal data systems, need a Ministry licence, and the system must be registered before it processes data.
- **Minimise biometrics.** Facial images, fingerprints and signatures need a legal basis or consent and prompt destruction; the state platform keeps no raw biometric images.
- **Plan for foreign users and data location.** Non-residents without Azerbaijani documents obtain signature credentials through embassies and consulates, and cross-border transfer of identity data is restricted.

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, including NFC reading of chip identity cards, for services that need a check outside the state login.
- Biometric liveness and face match for remote registration and account recovery flows.
- E-signatures and configurable no-code workflows that route high-value actions to stronger authentication.
- Cloud, on-premises or hybrid deployment to meet data location and cross-border transfer restrictions.

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

- **Azərbaycan Respublikası vətəndaşının şəxsiyyət vəsiqəsi haqqında Qanun [Law on the Identity Card of a Citizen of the Republic of Azerbaijan]** (14 June 1994, as amended), Articles 3 and 4, e-qanun, e-qanun.az/framework/9009
- **İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında Qanun [Law on Information, Informatisation and Protection of Information]** (3 April 1998, as amended), Articles 14, 14-1 and 14-2, e-qanun, e-qanun.az/framework/3525
- **Law No 1193-VIQD of 28 June 2024** amending the Family Code and the Identity Card, Information and Personal Data Laws (in force 16 July 2024), Milli Məclis, meclis.gov.az
- **Elektron imza və elektron sənəd haqqında Qanun [Law on Electronic Signature and Electronic Document]**, No 602-IIQ of 9 March 2004, Articles 1, 3, 11 and 33, e-qanun, e-qanun.az/framework/5916
- **Presidential Decree No 65 of 26 May 2004** on applying the E-signature Law, paragraphs 2.3 and 2.4, e-qanun, e-qanun.az/framework/5946
- **Presidential Decree No 1598 of 12 September 2017**, Rules of issuing electronic signature certificates to non-residents through diplomatic missions and consulates of the Republic of Azerbaijan (paragraphs 1.2 and 2.3 to 2.12), e-qanun, e-qanun.az/framework/36462
- **Dövlət xidmətləri haqqında Qanun [Law on Public Services]**, No 279-VIIQ of 31 October 2025 (in force 3 December 2025), e-qanun, e-qanun.az/framework/60932
- **Law No 494-VIIQD of 16 October 2026** on amendments in connection with the Law on Public Services (in force 28 October 2026), e-qanun, e-qanun.az/framework/62819
- **Presidential Decree No 472 of 12 August 2025** and the Regulation on the Electronic Government Information System, paragraphs 1.4, 3.4 to 3.8, 3.14 and 4.3 (as amended by Decrees No 575, 620 and 725 of 2026), e-qanun, e-qanun.az/framework/60355
- **Cabinet of Ministers Decision No 241 of 4 August 2025**, Rules on organising and providing electronic services, paragraph 2.11, e-qanun, e-qanun.az/framework/60431
- **Cabinet of Ministers Decision No 361 of 27 October 2026** amending Cabinet acts in connection with EGIS (in force 28 October 2026), e-qanun, e-qanun.az/framework/62848
- **Fərdi məlumatlar haqqında Qanun [Law on Personal Data]**, No 998-IIIQ of 11 May 2010, Articles 7.4, 8.6, 9, 14 and 15, e-qanun, e-qanun.az/framework/19675
- **Presidential Decree No 361 of 13 December 2010**, paragraph 3, e-qanun.az/framework/21035
- **Lisenziyalar və icazələr haqqında Qanun [Law on Licences and Permits]**, No 176-VQ of 15 March 2016, Annex 2, e-qanun, e-qanun.az/framework/32626; Ministry of Digital Development and Transport, licences in communications and IT, mincom.gov.az
- **Biometrik informasiya haqqında Qanun [Law on Biometric Information]**, No 651-IIIQ of 13 June 2008, Article 5.1, e-qanun, e-qanun.az/framework/15144
- **İnformasiya əldə etmək haqqında Qanun [Law on Access to Information]**, Article 26, e-qanun, e-qanun.az/framework/11142

- **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, Articles 1.1.7 to 1.1.9 and 3.1, e-qanun, e-qanun.az/framework/53369
- **İnzibati Xətalar Məcəlləsi [Code of Administrative Offences]**, Article 375, e-qanun, e-qanun.az/framework/46960
- **Unified Court Portal (courts.gov.az)**, anonymised decisions, administrative offence cases under Code of Administrative Offences Article 375, courts.gov.az
- **Presidential Decree No 676 of 2 June 2026** on improving cybersecurity governance, establishing the National Cybersecurity Agency and approving its Charter (paragraphs 3.1.24 to 3.1.26), e-qanun, e-qanun.az/framework/61938
- **Law No 431-VIIQD of 30 June 2026** on age-restricted social network platforms (applies from 5 August 2027), Milli Məclis, meclis.gov.az; status, e-qanun.az/framework/62377
- **Law No 454-VIIQD of 14 July 2026** amending the Law on Information, Informatisation and Protection of Information (State CERT (GOV CERT) duties; in force 10 August 2026), Milli Məclis, meclis.gov.az
- **Presidential Order No 1048 of 26 May 2026**, State Programme on expanding financial inclusion for 2027 to 2030, e-qanun, e-qanun.az/framework/61909
- **mygov ID**, frequently asked questions; mygov and mygov ID Privacy Policy and Unified Terms of Use (paragraph 3.2; Annex No 02, paragraph 2.1), IDDA, mygovid.gov.az/intro/faq, mygovid.gov.az (terms)
- **Cabinet of Ministers Decision No 323 of 30 October 2025**, Regulation on the "Highly Qualified Migrant" portal, paragraph 1.7.4, e-qanun, e-qanun.az/framework/58696
- **ASAN İmza**, first-time application and online renewal, asanimza.az; State Tax Service, "ASAN imza" (ASAN Certification Services Center), taxes.gov.az/en/page/asan-imza, and user instructions for certificate services, taxes.gov.az
- **State Tax Service**, "SİMA İmza identification methods (face recognition) to be used in electronic registration" (15 March 2024), taxes.gov.az
- **Ministry of Digital Development and Transport**, "digital.login to continue as MyGov ID" (28 October 2025), mincom.gov.az; "ESS launches project on personal data protection" (26 May 2026), mincom.gov.az
- **ASAN service**, issue and replacement of identity cards, asan.gov.az