Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Armenia

COUNTRY Armenia

INDUSTRY Telecom & Mobile Services

LAST UPDATED 13 November 2026

KEY REGULATORS Public Services Regulatory Commission · Ministry of High-Tech Industry and Artificial Intelligence · Personal Data Protection Agency of the Ministry of Justice

Key takeaways

- Running a mobile network in Armenia needs a network licence from the Public Services Regulatory Commission (PSRC); a provider that neither owns nor operates a network, such as a reseller, only has to notify the PSRC and can start five working days later.
- Every prepaid and postpaid SIM is issued under a paper or electronic contract that records the customer's name and identity document number, plus the registered address unless the customer presents a national ID card. Operators must keep these records in a database for three years after the contract ends.
- The rules let operators sign SIM contracts remotely through their own website or app, once the PSRC (after hearing the national security authority) has approved the app's design. For Armenian citizens the design must include a check against the State Population Register; foreign nationals can sign up online for internet access only.
- Telecom operators are not covered by Armenia's anti-money laundering (AML) law. A selfie or liveness check is biometric processing that needs documented consent and prior notification to the Personal Data Protection Agency, and an individual moving a number to another operator must present an identity document, whose details the losing operator matches against its records.
- A government bill to register every mobile phone's IMEI (device identifier) and bar unregistered phones from networks is before Parliament. It is not yet law: committee review was postponed on 30 September 2026, and Parliament's own experts have questioned its proposed 1 January 2027 start date.

Armenia's mobile market is served by three network operators (Telecom Armenia, Viva Armenia and Ucom), and it is open to new entrants, including providers that do not run their own network. The PSRC licenses networks, supervises service providers and sets the SIM contract rules; the Ministry of High-Tech Industry and Artificial Intelligence leads the pending device registration bill; and the Personal Data Protection Agency of the Ministry of Justice oversees how subscriber data is handled.

The biggest obstacle for a digital-first entrant is the approval step for online sign-up: an app or website that concludes SIM contracts must be agreed with the PSRC in advance, and every later change to it as well. Physical presence also matters: providers need a staffed customer office in every geographic area the PSRC defines.

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

Regulator	Remit	Level	Official site
Public Services Regulatory Commission (PSRC)	Network licences, radio frequency permits and numbering (art. 5), service notifications, number portability, SIM contract and archive rules, approval of online sign-up apps, consumer rules, penalties	National	psrc.am
National security authority	Gives its position on operators' online sign-up apps before the PSRC approves them	National	PSRC Decision 285-N (ARLIS)
Ministry of High-Tech Industry and Artificial Intelligence	Government lead on the IMEI registration bill (its minister is the bill's main rapporteur)	National	hightech.gov.am
Personal Data Protection Agency of the Ministry of Justice	Acts independently (art. 24(2)); checks compliance with the Law on Protection of Personal Data, applies administrative sanctions and receives mandatory notifications before biometric processing (arts. 23(3), 24)	National	dataprotection.moj.gov.am

National Assembly	Adopts amendments to the Law on Electronic Communications	National	parliament.am

Sector policy belongs to the "competent body" in article 4 of the telecom law. The Central Bank of Armenia and its Financial Monitoring Center supervise AML compliance, but only for the reporting entities the AML law lists; telecom operators are not among them.

2 Licensing and authorisation

The Law on Electronic Communications («Էլեկտրոնային հաղորդակցության մասին», 8 July 2005, last amended 3 July 2025) sets two routes into the market.

Network licence

No one may own or operate a public electronic communications network in Armenia without a network licence granted under the complex licensing procedure of the Law on Licensing (art. 15(2)). Use of radio frequencies needs a separate permit; the PSRC sets the procedures for licences, number assignments and frequency permits and grants them (art. 5).

Notification

A provider of public services that does not own or operate a network must notify the PSRC in writing, on the PSRC's standard form, and may start five working days after filing (art. 8.1(1)-(2)).

The law defines a network as a transmission system and, where applicable, the switching or routing equipment and other resources that carry signals (art. 2). A mobile virtual network operator (MVNO) that runs its own switching equipment therefore needs to assess whether it operates a network; one that only resells another operator's service uses the notification route.

Providing services without a licence or notification is prohibited (art. 15(3)). Continuing to provide services without a notification after a PSRC cease order is fined AMD 1,000,000 to 2,000,000 (art. 63(10)).

3 Identity framework (AML rules do not apply)

The Law on Combating Money Laundering and Terrorism Financing (26 May 2008) lists its reporting entities in article 3(1)(4), including banks, money transfer providers, insurers, crypto-asset service providers, gambling organisers and listed professions. Electronic

communications operators are not on the list; a telecom group that also transfers money is covered for that activity only.

Identity in the telecom sector is governed instead by sector rules, chiefly a PSRC decision adopted, in its own words, out of the need to protect public and national security interests:

- **SIM contract records.** PSRC Decision 285-N of 8 June 2011 (current version in force since 26 September 2025) applies to every prepaid and postpaid mobile SIM contract. Within five working days of signing, the operator must enter the contract in a paper and electronic, or electronic-only, database, including a scanned copy or, for contracts signed electronically, the electronic original (pt 1).
- **Number portability.** The PSRC's mobile number portability rules (Decision 251-N of 17 July 2013) require an identity document from every individual who ports a number, and a match against the losing operator's records (see section 4).
- **Confidentiality and data protection.** Customers' personal data and usage are confidential (Law on Electronic Communications, art. 49(1)), and the Law on Protection of Personal Data governs every document copy and selfie (see section 6).

4 Identity verification and onboarding

Data recorded for each SIM. For an individual: name, surname, identity document number, signature and registered address (the address is not stored if a national ID card is presented); for a legal entity: name, registration or taxpayer number and the authorised signatory. The record also notes where and when the contract was signed, or that it was signed through the operator's website or app, and the employee or agent who signed it (Decision 285-N, pts 2-3). Activation and termination dates are entered within five working days (pt 4).

Agents. An intermediary such as an agent may sign contracts; the record names it, and the operator stays responsible (pts 2(3), 6).

Number porting. An individual porting a number presents an identity document and gives name, surname, date of birth and document details (Decision 251-N, pt 26). The donor operator must accept if any one of five data combinations matches its records, including number plus document details alone (pts 30-32). It must answer 98% of requests within four working hours; silence counts as acceptance (pt 34).

Electronic signature. A document protected by an electronic digital signature has the same legal force as a handwritten signed document, if the signature is authenticated and the document is unaltered (Law on Electronic Document and Electronic Digital Signature, art. 4). The certificate on the national ID card is valid for the card's validity period (art. 14),

but only cards issued before 15 February 2023 carry the chip needed to sign or log in; holders of other cards use Mobile ID.

Mobile ID: an operator identity duty. Mobile ID is an electronic signature carried on a new-generation SIM or eSIM. Under Government Decision 572-N, annex 2 (restated 24 July 2025), ID-card holders obtain it by buying or replacing a SIM, or getting an eSIM, at offices of operators contracted to the signature operator (pt 12); foreign residents are first identified in person at the Migration and Citizenship Service (pt 13). The national services portal says Team Telecom, Ucom and Viva reissue the SIM against an ID card, with or without a chip, registered in the applicant's name. The operator's counter check therefore protects the holder's signing credentials.

Biometrics. No telecom rule requires face match or liveness detection. Where used, they need consent (Law on Protection of Personal Data, art. 13) and prior notification to the Agency (art. 23(3)); see section 6.

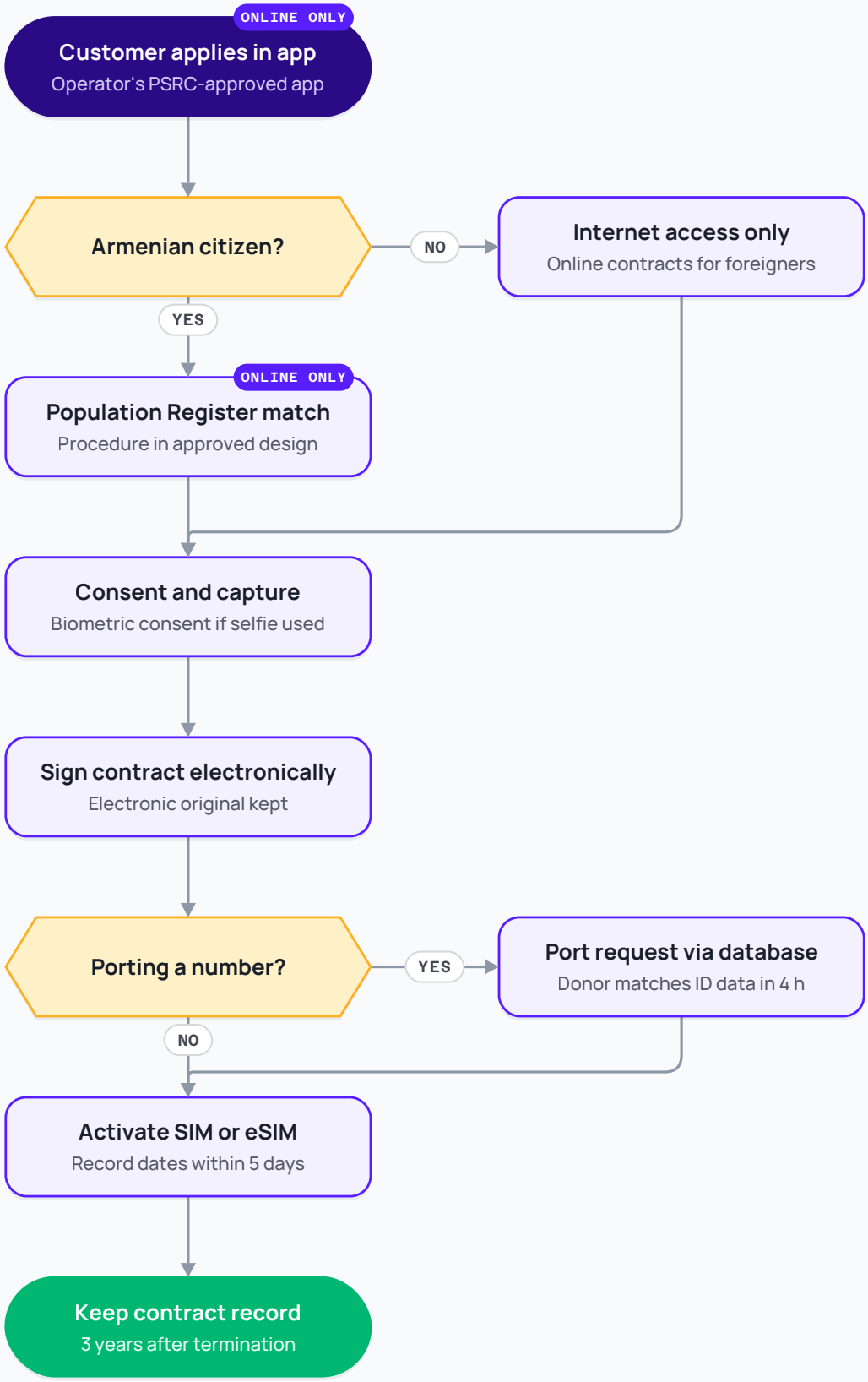


Figure 1. Remote SIM or eSIM activation through an operator's approved app in Armenia.

5 Digital channels: what's different

Bottom line: the rules provide for online SIM contracts through the operator's own website or app, after the PSRC has approved its design with input from the national security authority, and that design must check Armenian citizens against the State Population Register.

Requirement	In person / land-based	Online / remote	Difference
Who may sign the contract	Operator office or agent	Operator's own website or app	Differs
Prior approval of the channel	None	PSRC approval of app design and every change	Differs
Identity check against state data	Not specified	Population Register match for citizens	Differs
Foreign customers	All services	Internet access services only	Differs
Data recorded and kept	Same data; scanned copy, or electronic original if signed electronically	Same data; electronic original	Same
Biometric checks	Consent needed if used	Consent needed if used (selfie, liveness)	Same
Number porting	ID document and application	Same data; no channel named	Same
Customer office	Required in each PSRC area	Still required	Same

Approval of the sign-up app

The operator must agree the app's technical design, and every later change, with the PSRC, which consults the national security authority and may set minimum security conditions (Decision 285-N, pts 1.2-1.4). The design must include matching of Armenian citizens against the State Population Register; contracts with foreign nationals through the app may cover internet access only (pts 1, 1.2). The register check came with Decision 224-N (in

force 9 July 2024); Decision 320-N (in force 26 September 2025) limited it to citizens and added the foreign-national rule.

Pending: device registration

The IMEI bill `Bill, not enacted` would require operators to refuse or suspend service to unregistered mobile phones and to give the registry administrator subscribers' personal data with IMEI and SIM or eSIM numbers.

6 Data protection and biometrics

The Law on Protection of Personal Data (HO-49-N, 18 May 2015) applies to all identity data an operator captures. Four sets of provisions shape onboarding design:

- **Minimum data.** Data must be processed in the minimum volume needed for a lawful purpose, and processing is prohibited where the purpose can be achieved with depersonalised data (art. 5(2), 5(4)). Data no longer needed must be destroyed or blocked (art. 19(1)).
- **Legal basis and form of consent.** Consent is deemed given where the operator received the data under a contract with the data subject and uses it for that contract (art. 9(4)(2)), and data may be processed without consent where a law directly provides for it (art. 9(5)). Biometric data, however, need consent as such (art. 13), and the law sets its form: in writing, or electronically certified with an electronic digital signature, or, if oral, through reliable actions that clearly show it (art. 9(7)). The operator must prove consent was obtained (art. 9(8)), so a tick-box alone may not be enough for a selfie check.
- **Biometrics.** Biometric data only with consent, subject to the narrow statutory exception (art. 13), and only after notifying the Agency of the intended processing (art. 23(3)). Biometric data held outside information systems must be stored on media and with technologies that protect it; the autonomous body under the Law on Public Information sets those requirements (art. 19(6), as amended with effect from January 2026).
- **Security and leaks.** Operators must use encryption to protect information systems holding personal data and limit access to those entitled to it (art. 19(2)-(3)). If personal data leaks from an electronic system, the operator must publish a statement immediately and report the leak to the Police and the Agency (art. 21(4)).

Retention. SIM contract data are kept for three years after the contract ends (Decision 285-N, pt 5), and contract versions and change notices are archived for three years

(Decision 367-N, pt 1(4)); otherwise data may not be kept longer than their purpose requires (art. 5(5)).

Disclosure. Confidential customer data may be disclosed only in the cases article 49(2)-(2.2) of the Law on Electronic Communications lists, such as investigations under the procedure set by law, written customer consent, credit bureaus and emergency calls.

7 Sector-specific obligations

Number portability

Number portability has been available since 1 April 2014 (Decision 251-N, pt 2); unless the subscriber picks a later date, the number moves on the working day after the donor accepts (pt 35).

Contract changes and notices

Providers publish their terms and tariffs online. Adverse changes must be notified by SMS, email, automated call or TV message and take effect 30 days later, with a free right to terminate; for automatically renewing fixed-term contracts, expiry must be notified at least five days ahead, with free exit for at least 30 days after renewal (Decision 367-N, pts 1-2.1, as amended by Decision 237-N from 1 November 2025).

SIM replacement and eSIM

As at November 2026, apart from the Mobile ID arrangements above, no PSRC decision or other regulation sets identity checks for replacing a SIM or moving a number to a new SIM or eSIM; Decision 285-N sets records for SIM contracts but says nothing on replacements. The governing rule is the confidentiality duty in article 49, which a replacement issued to the wrong person would breach. For Mobile ID, Decision 572-N annex 2 provides for eSIM as well as SIM (pts 12, 14-15), and the national services portal says eSIM Mobile ID is issued at operators' service centres.

Subscriber requests for usage details

From 1 December 2026, on written or electronic request, an operator must give a subscriber up to one year of call, SMS, internet, roaming and paid third-party service details, including numbers, times, locations and charges, free when sent electronically (PSRC Decision 249-N of 9 September 2026, annex pts 2-5) `Adopted, effective 1 Dec 2026`. It does not say how the requester is authenticated; releasing this history to the wrong person would breach article 49.

Lawful interception and martial law

Operators must provide technical systems for authorised communications surveillance on request (Law on Operative-Investigative Activity, art. 26(3)). Under martial law, special rules on the use of means of communication may be set (Law on the Legal Regime of Martial Law, art. 8(1)).

8 Risk indicators and red flags

IDENTITY-ABUSE INDICATORS FOR MOBILE OPERATORS

- **Register mismatch**: an online applicant whose details do not match the State Population Register record.
- **Agent clusters**: many SIM contracts signed through one agent with the same identity document or address.
- **Late records**: contracts or activations not entered in the database within five working days.
- **Partial-match port requests**: a port accepted on document details alone, with name or birth date missing or different.
- **Unanswered port requests**: requests left past four working hours, which count as accepted.
- **Mobile ID SIM reissue**: a request to reissue a SIM or eSIM with Mobile ID, which would transfer the holder's signing credentials to the new card.
- **Data requests without a legal basis**: callers or emails seeking call or location data outside the cases in article 49.

9 Enforcement and penalties

The PSRC enforces the law and its own decisions (art. 63), with penalties tiered by breach and by annual telecom turnover (AMD 500 million is the dividing line). The operator is responsible for the SIM contract rules (Decision 285-N, pt 6).

Breach	Turnover up to AMD 500m	Turnover above AMD 500m

Breach of the law, first instance (no aggravating effect)	Warning	Warning
Breach of the law harming a group of consumers, gross licence breach, breach of customer confidentiality, or a repeat within one year	AMD 1m to 2m, or licence suspension or termination	AMD 20m to 40m, or licence suspension or termination
Breach of a PSRC decision, first instance	Warning	Warning
Breach of a PSRC decision with the same aggravating effects, or a repeat	AMD 500,000 to 1m, or licence suspension or termination	AMD 10m to 20m, or licence suspension or termination

If a requirement is in both, the law's penalty applies (art. 63(11)).

Recent action. By Decision 347-A of 8 October 2025, the PSRC fined Telecom Armenia AMD 10,000,000 under article 63(9) for breaching points 20 and 25 of its licence conditions, in a case about free duct capacity requested by another operator. Telecom Armenia challenged the decision in the Administrative Court, and the PSRC reported the case as pending at the end of 2025.

10 Recent changes and what to watch

- **1 December 2026:** `Adopted, effective 1 Dec 2026` PSRC Decision 249-N: subscribers can request up to a year of call, SMS, internet and location details, free when delivered electronically.
- **30 September 2026:** `Bill, not enacted` Committee review of the IMEI registration bill (K-7-12.08.2026) postponed. Parliament's experts had flagged a Tax Code conflict with the 1 January 2027 start and loosely defined personal data provisions.
- **12 August 2026:** `Bill, not enacted` Government submits the IMEI bill. Operators would have to check IMEI compliance before serving a phone and share subscriber data with a registry administrator founded jointly by the mobile operators.
- **1 November 2025:** `In force` PSRC Decision 237-N: five-day expiry notice and free exit after automatic renewal of fixed-term contracts.
- **26 September 2025:** `In force` PSRC Decision 320-N: online contracts with foreign nationals limited to internet services; Population Register check limited to Armenian citizens; PSRC may set security conditions for sign-up apps.

- **9 July 2024:** `In force` PSRC Decision 224-N allows SIM contracts through operators' websites and apps, once PSRC approves a design that includes a Population Register check.

11 What this means for identity verification

- **Build inside the operator's own channel.** Verification must be part of the app design the PSRC approves; changes need fresh approval.
- **Add the Population Register check.** Match citizens against the register; route foreign nationals to internet-only plans online.
- **Capture the fields the rules name.** Name, surname, registered address (unless the ID card is used), identity document number, and the date of birth the porting rules match on.
- **Separate consent for biometrics.** Notify the Agency first; capture consent in a form that meets art. 9(7), with a fallback for customers who refuse.
- **Guard SIM reissues.** Treat any SIM or eSIM replacement, above all one carrying Mobile ID, as an identity event.
- **Keep the electronic original.** Store the signed contract with encryption and backups for three years after termination.
- **Prepare for device data.** If the IMEI bill passes, activation will need to link subscriber, SIM or eSIM and IMEI.

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 SIM and eSIM onboarding inside the operator's own app, with ID document capture and verification, including NFC reading of passports and chip-bearing Armenian ID cards.
- Face match and biometric liveness checks with a documented consent step built into the activation flow.
- Accurate capture of the contract fields the PSRC rules name, plus the date of birth that number porting matches on.
- E-signatures for remote subscriber contracts, with an audit trail for each check.
- No-code workflow builder and on-premises or hybrid deployment to fit a design submitted for PSRC approval.

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

- **Law on Electronic Communications** («Էլեկտրոնային հաղորդակցության մասին» օրենք, HO-176-N, 8 July 2005, amended up to 3 July 2025), arts. 2, 4, 5, 8.1, 15, 46, 49, 63, ARLIS, arlis.am/hy/acts/209934
- **PSRC Decision 285-N of 8 June 2011, Standards for keeping archives of contracts for prepaid and postpaid mobile phone cards** (amended up to Decision 320-N of 17 September 2025; online contracting added by Decision 224-N of 3 July 2024), ARLIS, arlis.am/hy/acts/212855
- **PSRC Decision 251-N of 17 July 2013, Rules on the mobile number portability service** (amended up to 11 June 2014), pts 2, 26-35, ARLIS, arlis.am/hy/acts/91517

- **PSRC Decision 367-N of 25 October 2023, on notifying subscribers of changes to and expiry of subscriber contracts and archiving the documents** (amended by Decision 237-N of 2 July 2025), ARLIS, arlis.am/hy/acts/215203
- **Law on Protection of Personal Data** («Անձնական տվյալների պաշտպանության մասին» օրենք, ՀՕ-49-Ն, 18 May 2015), arts. 5, 9, 13, 19, 21, 23, 24, ARLIS, arlis.am/hy/acts/229131
- **Government Decision 572-N of 25 May 2017** on the use of electronic documents and electronic digital signatures in state bodies, annex 2 (restated by Decision 1026-N of 24 July 2025), pts 12-15, ARLIS, arlis.am/hy/acts/209938
- **What is the "YesEm" Identification Platform and How to Log in?**, National Services Gateway (Hartak), english.hartak.am
- **Personal Data Protection Agency**, dataprotection.moj.gov.am
- **Law on Electronic Document and Electronic Digital Signature** (14 December 2004), arts. 4, 14, ARLIS, arlis.am/hy/acts/218694
- **Law on Combating Money Laundering and Terrorism Financing** (26 May 2008), art. 3(1)(4), ARLIS, arlis.am/hy/acts/210014
- **Law on Operative-Investigative Activity**, art. 26(3), ARLIS, arlis.am/hy/acts/224811
- **Law on the Legal Regime of Martial Law**, art. 8(1), ARLIS, arlis.am/hy/acts/215194
- **Draft law K-7-12.08.2026-ՏՀ-011/0 amending the Law on Electronic Communications (IMEI registration)**, text, justification, expert opinion of 4 September 2026 and consideration history, National Assembly, parliament.am
- **PSRC Decision 249-N of 9 September 2026, Procedure for providing subscribers with information on services provided by operators** (in force 1 December 2026), PSRC electronic library, psrc.am
- **PSRC Decision 347-A of 8 October 2025, on fining Telecom Armenia OJSC**, PSRC electronic library, psrc.am
- **PSRC information on court cases involving the Commission in 2025** (19 December 2025), psrc.am, annual reports page
- **PSRC 2025 annual report** (April 2026), section 4, psrc.am, annual reports page