



Identomat

COMPLIANCE GUIDE

Telecom & Mobile Services Compliance in Georgia

COUNTRY Georgia

INDUSTRY Telecom & Mobile Services

LAST UPDATED 16 October 2026

KEY REGULATORS Georgian National Communications Commission · State Audit Office of Georgia · Operational-Technical Agency of the State Security Service of Georgia

Key takeaways

- Anyone offering mobile, fixed or internet services in Georgia must first register with the Georgian National Communications Commission (GNCC); registration is granted within 10 working days and foreign companies have the same rights as Georgian ones.
- Telecom operators are not covered by Georgia's anti-money laundering (AML) law, but every subscriber must be identified by name, surname and personal number before a SIM card or number is issued.
- Selling a SIM or eSIM online is allowed for adults and companies, but the operator must identify the customer through an identity document read electronically, a bank-verified payment, or an identity document combined with a visual check.
- Since 4 September 2026 operators may check applicants against the state identity database and refuse contracts that do not match; existing subscribers can be re-checked until early March 2027 and disconnected if they do not correct their data.
- Using selfies or face matching to verify customers means processing biometric data, which Georgian law allows only when strictly necessary, documented in advance and usually backed by written consent.

Georgia is open to new telecom entrants, including mobile virtual network operators (MVNOs): authorisation is a registration rather than a discretionary licence, and since July 2024 the largest mobile operator must give MVNOs access to its network. Remote, app-based onboarding is expressly permitted for both new subscriptions and number porting.

The Georgian National Communications Commission regulates the sector. The State Audit Office supervises personal data protection, and the Operational-Technical Agency of the State Security Service sets technical lawful-access requirements that every telephone or internet provider must meet before launch.

The biggest practical obstacle for a new entrant is not identity verification but launch readiness: an operator must show the Commission 14 days before starting service that its lawful-interception, data-retention and, for mobile networks, device-blocking capabilities meet Georgian requirements.

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 relevant to telecom onboarding	Level	Official site
Georgian National Communications Commission (GNCC)	Authorisation, spectrum and numbering, consumer and subscriber-identification rules, number portability, sanctions	National, independent regulator	comcom.ge
State Audit Office of Georgia	Personal data protection supervision, including telecom data disclosures to law enforcement	National	pdp.sao.ge
Operational-Technical Agency of the State Security Service of Georgia	"Authorised body" for lawful interception, data copying and real-time geolocation	National	ota.gov.ge
Public Service Development Agency of the Ministry of Justice	Keeper of the identity database operators may check applicants against	National	sda.gov.ge
Financial Monitoring Service of Georgia	Receives notifications on assets of UN-sanctioned persons (all businesses, not only AML-obliged entities)	National	fms.gov.ge

Georgia is a unitary state, so authorisation is national. The Commission is the single regulator of electronic communications under Article 5 of the [Law of Georgia on Electronic Communications](#).

2

Licensing and authorisation

Authorisation by registration. Providing public electronic communication networks or services requires authorisation, which is a registration in the Commission's departmental registry under Articles 14 to 18 of the Law on Electronic Communications **In force**. The Commission must register an applicant within 10 working days, the authorisation has no expiry date, and activity may begin from the day of registration. Article 3(2) gives foreign citizens and companies the same rights and duties as Georgian businesses.

Scarce resources. Spectrum is used under a licence and numbers under a separate permit for numbering resources; both are granted by the Commission. MVNOs rely on wholesale access: on 25 July 2024 the Commission designated Magticom as having significant market power in mobile services and required it to offer national roaming, co-location and MVNO access, with the decision to be reviewed after three years ([GNCC announcement, 25 July 2024](#)).

Pre-launch technical conditions. Article 19(2¹)(e) requires an electronic communications company, 14 days before starting authorised activity, to confirm to the Commission that its real-time interception capability, data-copying arrangements and IT infrastructure meet Georgian requirements. Mobile operators must also confirm real-time geolocation capability and the ability to detect and block stolen handsets through the unified mobile equipment search system (Article 19(2¹)(d)).

Ongoing duties. Authorised persons pay a regulatory fee of 0.75 per cent of regulated revenue excluding VAT, filed monthly (Article 12(4)); notify changes in activity or shareholders within seven working days (Article 19(2)©); and notify the Commission before any acquisition that brings a holder to 5 per cent or more of their shares (Articles 25 and 26). Providers must also register on the My.gov.ge e-services portal within 15 days of authorisation (Article 4(4) of the Commission's consumer regulation).

Identity framework (AML rules do not apply)

Telecom operators are not obliged entities. Article 3 of the [Law of Georgia on Facilitating the Prevention of Money Laundering and the Financing of Terrorism](#) lists financial institutions, certain professions, gambling organisers, dealers in precious metals and two public bodies; electronic communications providers are not among them. There is therefore no customer due diligence, suspicious transaction reporting or AML record-keeping duty for selling connectivity.

Two AML-law provisions still reach every business. Under Articles 1(3) and 41(7) to (8), all natural and legal persons must not make funds or other property available to persons on UN Security Council sanctions lists and must notify the Financial Monitoring Service when they apply such a restriction; a repeated failure carries a GEL 1,000 fine under Article 43¹, added by Law No. 1119 of 26 November 2025 **In force**.

Identity in telecom is instead governed by three instruments:

Law on Electronic Communications

Defines a subscriber as an end-user served under a prior written contract; sets confidentiality, retention and lawful-access duties.

GNCC Resolution No. 3 of 2006

Consumer regulation setting contract content, the identification methods for distance contracts and the data operators must hold on each customer.

GNCC Resolution No. 3 of 2010

Number portability regulation, including remote porting requests and identification of the person receiving the new SIM or eSIM.

Identity verification and onboarding

What must be collected. The consumer regulation (GNCC Resolution No. 3 of 17 March 2006, as amended by [Resolution No. 2 of 20 April 2021](#), in force 1 January 2022) requires every contract to state the subscriber's identifying and contact data. Identifying data means name, surname and personal number for individuals, and name, form and identification code for companies (Article 3(1) (h16)). The provider must ensure the correct identification of customers whichever method it uses (Article 12(12)) and must let a customer see all numbers registered in their name (Article 12(13)).

Contracts and consent. Mobile telephone service is provided under a written (including electronic) contract or a distance contract (Article 10⁵(1)). Consent may be confirmed by a handwritten or qualified electronic signature, an "order and pay" button, a code word or a one-time code (Article 3(1)(h26)).

State database check. Since [GNCC Resolution No. 5 of 3 September 2026](#) took effect on publication (4 September 2026), a provider may verify the applicant's identifying data in the Public Service Development Agency database and may refuse a contract if the data (other than contact details) do not match and the applicant cannot be identified unambiguously (new Article 83(2¹)) **In force**.

Biometrics. The telecom rules do not require selfies, face matching or liveness checks; a provider that uses them must meet the biometric rules in section 6. No identity assurance level or presentation-attack standard is specified for telecom onboarding.

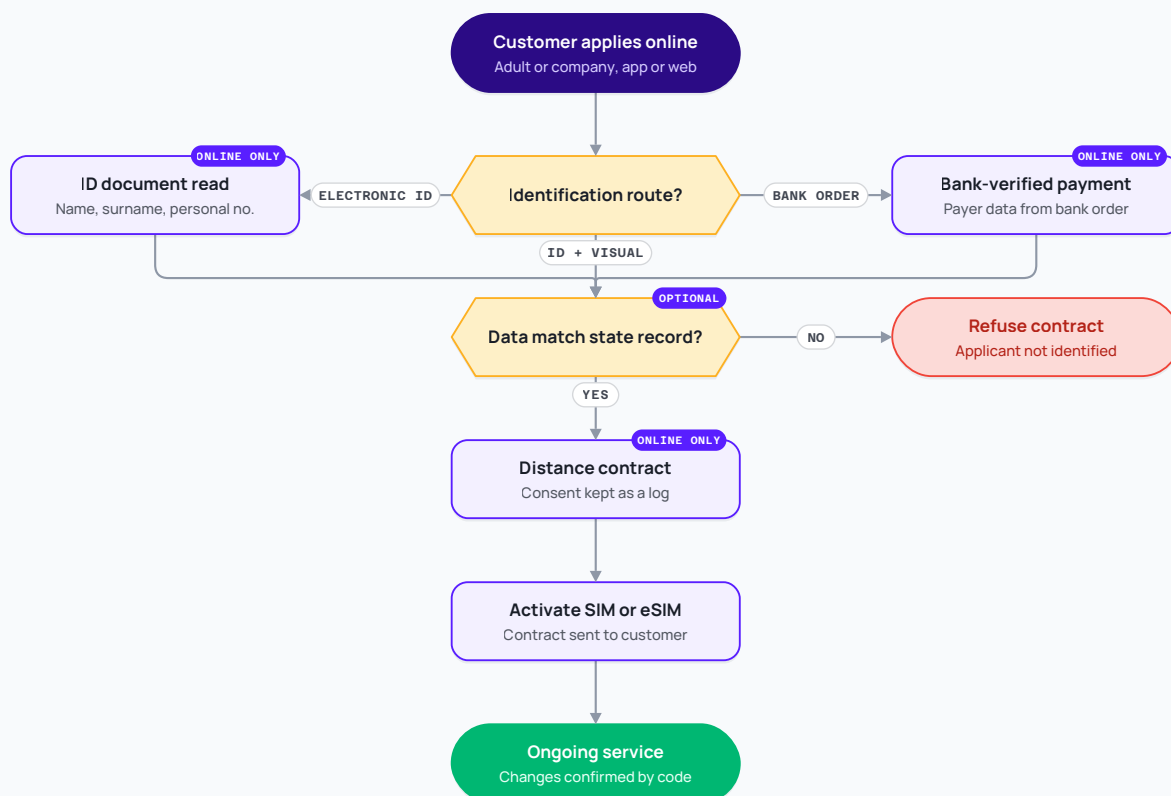


Figure 1. Remote SIM or eSIM onboarding under GNCC rules.

Bottom line: online SIM and eSIM sales are permitted, but a distance contract for a phone number or internet access must rest on one of three prescribed identification routes, and the operator must keep a log of the customer's consent.

Requirement	In person	Online / remote	Difference
Contract form	Written (including electronic) contract	Distance contract, with adults and legal entities only	Differs
Identification method	Correct identification of the customer	ID read electronically, bank-verified payment, or ID plus visual identification	Differs
State database check	Permitted; mismatch allows refusal	Permitted; mismatch allows refusal	Same
Evidence of consent	Signature on contract	Consent log in the form obtained, plus all later changes	Differs
Short internet access	Standard contract rules	Wireless access of up to three days exempt from the electronic-ID route	Differs
Number porting request	Written application	Website or app, completed with a code sent to the number	Differs
Identifying the SIM or eSIM recipient when porting	Consumer-regulation identification rules	Same rules, before eSIM handover	Same
Retention of subscriber data	4 years after contract ends	4 years after contract ends	Same

Three routes for a remote contract

Article 12(10) of the consumer regulation requires a distance contract for core services tied to the issue of a national number or to internet access to be concluded on the basis of

an identity document from which name, surname and personal number can be read electronically; for a company, the representative's document is used. Article 12(11) offers an alternative for customers with a current account at a Georgian commercial bank that has identified and verified them: the provider may rely on a standing or one-off payment order carrying the customer's name, surname, personal number and account details. Article 12(15) allows the provider to use neither mechanism if it identifies the customer from an identity document, identifies the customer visually, concludes the contract through a consent mechanism and delivers the contract in paper or electronic form. The regulation does not specify how visual identification is performed at a distance.

Consent records and disclosures

Before service starts, the provider must confirm the distance contract by a reliable electronic means (Article 12(7)). It must keep the contract and the customer's consent as a log in the form obtained, with every later change, the time and means of consent, and provide this to the customer free of charge (Article 12(9)), holding it no longer than necessary (Article 12(14)).

Remote porting

Under [GNCC Resolution No. 4 of 23 June 2022](#) (in force 1 January 2023), mobile operators must accept porting requests in writing and through a website or app, and remote requests are completed with a code sent to the number being ported. Porting must finish within 24 hours of registration in the central database, extendable to five working days by agreement where a physical SIM is delivered. The service contract must be concluded, and the SIM or eSIM handed over, at least one hour before porting completes, or the process stops.

6 Data protection and biometrics

The [Law of Georgia on Personal Data Protection](#) (No. 3144, 2023) applies to all identity capture, and the State Audit Office supervises it. Several provisions bite directly on telecom onboarding:

- **Biometrics are special-category data.** Facial images processed to identify a person uniquely are biometric data and a special category (Article 3(b) and (d)). Processing needs a ground in Article 6, typically written consent, plus the safeguards the law requires.
- **Necessity test.** Since 1 May 2026 ([Law No. 1259 of 17 December 2025](#)), Article 9(1) allows biometric processing for carrying out activities, security, property protection or preventing disclosure of secrets only where these purposes cannot be achieved by

other means without disproportionate effort. Article 9(2) requires the controller to set down in writing, before processing, the purpose, data volume, storage period, destruction rules and safeguards.

- **Impact assessment and officer.** A data protection impact assessment is mandatory when special-category data of a large number of people is processed (Article 31(2) (b)), and electronic communication companies must appoint a personal data protection officer (Article 33(1)).
- **Incidents and foreign providers.** Incidents must be notified to the State Audit Office within 72 hours (Article 29). A controller established outside Georgia that processes data using technical means in Georgia must appoint a special representative, unless it is established in the EU or an adequate country (Article 34).

Sector retention is set by Article 8⁵ of the Law on Electronic Communications: subscriber identity and contract data may be kept for no more than four years after the contract ends and must be destroyed automatically within 30 days of expiry. The consumer regulation aligns with this four-year period (Article 7, as amended by [Resolution No. 2 of 9 June 2022](#)).

7 Sector-specific obligations

Lawful access and disclosure records

Information on users and their communications is confidential (Article 8). The Operational-Technical Agency has stationary access for interception and may copy identification-data databases (Articles 8¹ and 8³). Providers must disclose identification data to investigators under Article 136 of the Criminal Procedure Code, record each transfer and inform the State Audit Office (Article 8²), which the data protection law requires within 24 hours of the transfer (Article 28(5)).

Lost SIMs, stolen devices and contract changes

The contract must state how and how quickly service is blocked when a SIM card is lost, and no fee may be charged for blocking (Article 10⁵(6) of the consumer regulation). Mobile operators must detect activation of stolen handsets and restrict them through the unified mobile equipment search system, and report the number, its owner, time and location to the investigating body (Article 19(2¹) (d) and (d¹) of the Law). Where a written or distance contract exists, the provider may add services, change the tariff plan or amend the contract on the customer's confirmation by the reliable method set in the contract, such as a code word or one-time code (Article 85(9)).

Porting safeguards

Porting is refused if the number belongs to someone else or its holder cannot be established, or if 30 days have not passed since the customer became a subscriber or last ported (Article 5(3) of the porting regulation). When a customer asks the donor operator by phone whether a number can be ported, the operator must identify them by the calling number and their personal number, and must refuse to answer if the details do not match its records (Article 3(10) and (12)).

8

Risk indicators and red flags

TELECOM IDENTITY-ABUSE INDICATORS DRAWN FROM GNCC RULES AND FINDINGS

- **SIM box use:** numbers issued without proper contracts used to convert international calls into local ones (GNCC, 2017).
- **Contract without ID or with false data:** test purchases at all three mobile operators succeeded in 2017.
- **Data mismatch with the state record:** applicant details that do not match the identity database.
- **Port-out request from an unmatched caller:** personal number does not match the holder of the number.
- **Rapid churn:** porting attempted within 30 days of activation or of a previous port.
- **Third-party SIM collection:** SIM or eSIM delivered to someone other than the number holder during porting.
- **Lost-SIM claims followed by changes:** blocking requests quickly followed by tariff or service changes.

9

Enforcement and penalties

Under Article 45 of the Law on Electronic Communications, the Commission may first issue a written warning for breach of electronic communications legislation, including its own resolutions. If a continuing breach is not cured within the deadline it sets, or a new breach occurs within a year, it may impose a fine of 0.5 per cent of the operator's income for the previous 12 months, paid to the state budget. Where a warning and a fine have already been applied for a breach, the Commission may suspend the authorisation until the breach

is remedied (Article 19¹(1)©). The State Audit Office may separately order processing to stop and impose administrative liability (Article 52 of the data protection law).

Identity-related actions: in September 2015 the Commission fined two mobile operators GEL 30,000 each for serving subscribers without written contracts after test purchases through dealers, and warned a third ([GNCC, 28 September 2015](#)). On 13 October 2017 it warned all three mobile operators after test purchases on 7 September 2017 showed contracts could be concluded without an identity document and with false personal data ([GNCC, 13 October 2017](#)).

10 Recent changes and what to watch

- **4 September 2026** **In force** GNCC Resolution No. 5 lets operators check applicants against the state identity database and refuse unmatched applicants; existing subscribers may be re-checked for six months (to early March 2027) and disconnected if they do not correct their data within 30 days of notice.
- **1 May 2026** **In force** Rewritten Article 9(1) of the data protection law narrows when biometric data may be processed; review face-match and liveness flows against the necessity test.
- **17 December 2025** **In force** The State Audit Office is the data protection supervisor named throughout the data protection law and receives notifications of telecom data transfers to law enforcement.
- **26 November 2025** **In force** AML law amendment (Law No. 1119) confirms that every business, including telecom operators, must not make assets available to UN-sanctioned persons and must notify the Financial Monitoring Service.
- **25 July 2024** **In force** Magticom must offer MVNO access, national roaming and co-location; the Commission will review the decision after three years.

11 What this means for identity verification

For app-based SIM and eSIM sales, the main design choice is which of the three identification routes to support. Reading the identity document electronically suits customers holding a chip-based Georgian document; the bank-payment route suits customers who pay from a Georgian bank account; and the document-plus-visual route covers everyone else, including foreign customers, but rests on a visual identification step whose remote form the regulation leaves to the operator.

The new database check makes the personal number the anchor field: capture it accurately, match it before activation, and record the reason for any refusal. If selfies or face matching are used, document necessity under Article 9, obtain written consent, run an impact assessment and set a deletion period no longer than the four-year sector limit. Port-out, eSIM transfer and contract changes are the points where re-verification matters most: confirm by code sent to the number, and identify any person collecting a SIM.

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 chip reading, to identify SIM and eSIM customers remotely by name, surname and personal number.
- Face match and biometric liveness for the document-plus-visual identification route, with configurable data retention.
- Phone and email verification and e-signatures to capture and log customer consent for distance contracts.
- AML screening against sanctions lists, to support the duty not to make assets available to UN-sanctioned persons.
- No-code workflow builder and an audit trail of every check, deployable in the cloud, on-premises or hybrid.

[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

- **ელექტრონული კომუნიკაციების შესახებ** [Law of Georgia on Electronic Communications], No. 1514, 2 June 2005, consolidated version of 10 June 2026, Articles 2, 3, 5, 8 to 8⁵, 12, 14 to 19¹, 25, 26, 45, Legislative Herald of Georgia, matsne.gov.ge
- GNCC Resolution No. 3 of 17 March 2006 on the regulation on service provision and consumer protection in electronic communications, document record, matsne.gov.ge
- GNCC Resolution No. 2 of 20 April 2021 amending Resolution No. 3 of 2006, Articles 3, 4, 10⁵, 12, 83 to 85, in force 1 January 2022, matsne.gov.ge
- GNCC Resolution No. 2 of 9 June 2022 amending Resolution No. 3 of 2006, Article 7 (data retention), matsne.gov.ge
- GNCC Resolution No. 5 of 3 September 2026 amending Resolution No. 3 of 2006, Article 83(2¹) and transitional Article 2, published 4 September 2026, matsne.gov.ge
- GNCC Resolution No. 3 of 6 July 2010 on the regulation on subscriber number portability, Articles 3 to 5, matsne.gov.ge
- GNCC Resolution No. 4 of 23 June 2022 amending the number portability regulation, in force 1 January 2023, matsne.gov.ge
- **ფულის გათვთრებისა და ტერორიზმის დაფინანსების აღკვეთის ხელშეწყობის შესახებ** [Law of Georgia on Facilitating the Prevention of Money Laundering and the Financing of Terrorism], No. 5226-ლ, 30 October 2019, consolidated version of 1 April 2026, Articles 1, 3, 41, 43¹, matsne.gov.ge
- Law of Georgia on Personal Data Protection, No. 3144-ქიშ-ქმპ, 14 June 2023, consolidated version of 10 June 2026, Articles 3, 6, 9, 28, 29, 31, 33, 34, 52, matsne.gov.ge
- Law No. 1259-IVმს-ქიშპ of 17 December 2025 amending the Law on Personal Data Protection (Article 9(1)), in force 1 May 2026, matsne.gov.ge
- GNCC, Magticom designated as operator with significant market power; access obligations imposed, 25 July 2024, comcom.ge
- GNCC, written warnings to Magticom, Beeline and Geocell for breach of subscriber contract rules, 13 October 2017, comcom.ge
- GNCC, warning to Magticom and GEL 30,000 fines on Mobitel and Geocell, 28 September 2015, comcom.ge