



Identomat

COMPLIANCE GUIDE

Government & Public Services Compliance in Georgia

COUNTRY Georgia

INDUSTRY Government & Public Services

LAST UPDATED 16 October 2026

KEY REGULATORS Public Service Development Agency · Digital Governance Agency · State Audit Office of Georgia

Key takeaways

- Georgia has no single digital identity law: the electronic ID card, the state population register and qualified electronic signatures together form the national identity framework.
 - A qualified electronic signature (the highest legal grade of e-signature) has the same legal effect as a handwritten one, and anyone filing a signed document with a public body online must use one; non-residents are exempt from that requirement.
 - Firms may treat identity data obtained lawfully from the state register as proof of identity, which is how most remote onboarding in Georgia is anchored.
 - Online, the most detailed rules come from the National Bank of Georgia for the firms it supervises: live selfie checks, matching against the state register photo, machine-read documents and a cap of three failed attempts a day.
 - Since 2 March 2026 the State Audit Office, not the former data protection service, supervises personal data; biometric checks need a written purpose and retention policy before they start.
-

Georgia's public sector is open to digital delivery and has been for more than a decade. Citizens and residents hold chip-based identity cards that carry an authentication certificate and a qualified signature certificate, and the Unified Portal of Electronic Services (my.gov.ge) gives access to public and private electronic services.

The principal authorities are the Public Service Development Agency, which keeps the population register and issues identity documents, and the Digital Governance Agency, which runs the portal and authorises trust service providers. Both operate under the Ministry of Justice. The State Audit Office supervises data protection.

The biggest obstacle for a new entrant is that there is no published assurance-level scheme for public services. A provider building identity checks for, or alongside, government services must assemble requirements from the identity card law, the trust services law, the data protection law and, where it is a regulated financial firm, the National Bank's remote onboarding rule.

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

Georgia is a unitary state, so identity documents, trust services and data protection are regulated nationally.

Authority	Remit for identity	Level	Official site
Ministry of Justice of Georgia	Policy owner; the Minister sets technical standards for identity cards and the authorisation rules for trust service providers	National	justice.gov.ge
Public Service Development Agency (PSDA)	Population register, identity cards, residence cards and passports; the electronic database used to verify identity	National	sda.gov.ge
Digital Governance Agency (DGA)	my.gov.ge, the state data exchange infrastructure, authorisation and supervision of qualified trust service providers	National	dga.gov.ge
Public Service Hall	In-person service delivery for Ministry of Justice services	National, branch network	psh.gov.ge
State Audit Office of Georgia	Personal data protection supervision, complaints, inspections and fines (from 2 March 2026)	National	pdp.sao.ge

Operational-Technical Agency of the State Security Service	Information security and cyber security powers over critical information system subjects	National	ota.gov.ge
National Bank of Georgia	Remote (electronic) customer identification rules for the financial firms it supervises	National	nbg.gov.ge

2 Licensing and authorisation

No licence is needed simply to verify identity or to integrate with public e-services. Two roles do require authorisation.

Qualified trust service providers

Under Article 11 of the Law of Georgia on Electronic Documents and Electronic Trust Services (as amended by Law No. 6298-III of 12 June 2020), anyone wishing to provide qualified trust services (qualified signatures, seals, time stamps and validation) must be authorised by the DGA. The application includes an audit report on compliance with the law and the Government's technical regulation, proof of civil liability insurance (or, for an administrative body, financial guarantees) and the provider's published internal regulations. The DGA checks compliance when necessary and at least once every two years, publishes the list of qualified providers and may suspend or revoke an authorisation. Under the DGA law the authorisation fee may not exceed GEL 20,000. **In force**

Access to the state register

Private access to register data is contractual. Article 20(4) of the Law on the Procedure for Registering Citizens of Georgia and Aliens Residing in Georgia, for Issuing an Identity (Residence) Card and a Passport allows the PSDA, under a contract with a business or non-commercial legal entity, to release registration and identity-document data with the data subject's consent. Consent is deemed given where it can be inferred from the nature of the action the requesting entity is performing for that person.

Foreign qualified trust services have legal force in Georgia only where Georgia has concluded an international agreement on their recognition (Article 12 of the trust services law).

Identity framework (AML rules do not apply)

Public-service delivery is governed by identity, electronic signature and data protection law, not by the anti-money laundering regime. Customer due diligence obligations arise only where a regulated financial or designated business relies on state identity data, and they bind that business, not the public body.

Primary identity documents

Article 11 of the identity card law names the citizen's identity card and the residence card as the primary documents proving identity. The citizen's passport proves identity and citizenship inside and outside Georgia (Article 20¹). Every citizen must obtain an identity card within six months of turning 14 (Article 3(2)).

The personal number

Each person receives a unique personal number on registration or document issue that may not be changed except where the law expressly allows (Article 1¹). It is the key that links register records, documents and electronic certificates.

Register as proof of identity

A party to a legal relationship that has lawfully obtained identity-card data from the PSDA database may use it to identify the person as an identity document. Any legal document showing a name, surname and personal number may be used for identification if the details are checked against the PSDA database (Article 11¹).

Electronic signatures

A qualified electronic signature has the same legal effect as a handwritten signature. Public bodies may not reject documents, or deny evidential value to signatures, solely because they are electronic or not qualified (Article 3(1), (6) and (7) of the trust services law).

Sanctions screening and politically exposed person checks are obligations of regulated firms, not of public bodies, and are outside this framework.

Identity verification and onboarding

The electronic identity card

Law No. 1120-IV⁰ბ-XI⁰ჯ of 26 November 2025, in force from 1 January 2026, restated Article 14 of the identity card law. The chip of the electronic identity (residence) card may hold a qualified electronic signature certificate and an authentication certificate, each with its own activation data protecting against unauthorised use. The card must carry the holder's

name, sex, citizenship, date and place of birth, personal number, photograph, signature specimen, a card access number (CAN), a QR code for checking the document or the person, and the holder's fingerprints. Cards may be issued without fingerprints where they cannot be taken for health or physical reasons. Cards issued before 2026 remain valid for their term, and applications filed before that date could still produce cards without fingerprints. **In force**

Adult identity cards are valid for 10 years and cards for under-18s for 4 years (Article 14(2)). Permanent residence cards run 5 years for adults; temporary residence cards follow the residence permit, capped at 5 years. Non-electronic identity cards issued before 28 July 2011 ceased to be valid on 1 July 2024 (Article 20¹⁵).

Two technical points matter for system design. The electronic card is expressly not an "electronic document" under the trust services law (Article 1¹(2¹)), so its chip data proves identity under the identity card law, not as a signed record. And the card does not show the address; residence is confirmed by checking the electronic card against the PSDA database (Article 2(4)).

Remote proofing benchmark

No public-sector act sets identity assurance levels. The most detailed published standard for remote proofing is National Bank Order No. 104/04 of 29 April 2025 (amended by Orders No. 142/04 and No. 288/04 in 2025), which binds firms supervised by the National Bank. It requires a consent step, a real-time liveness check and either a live document check or a comparison of the live photo with the photograph obtained from the PSDA database. Georgian identity cards, passports and residence cards must be checked against PSDA data, and document data must be read automatically by OCR or NFC.

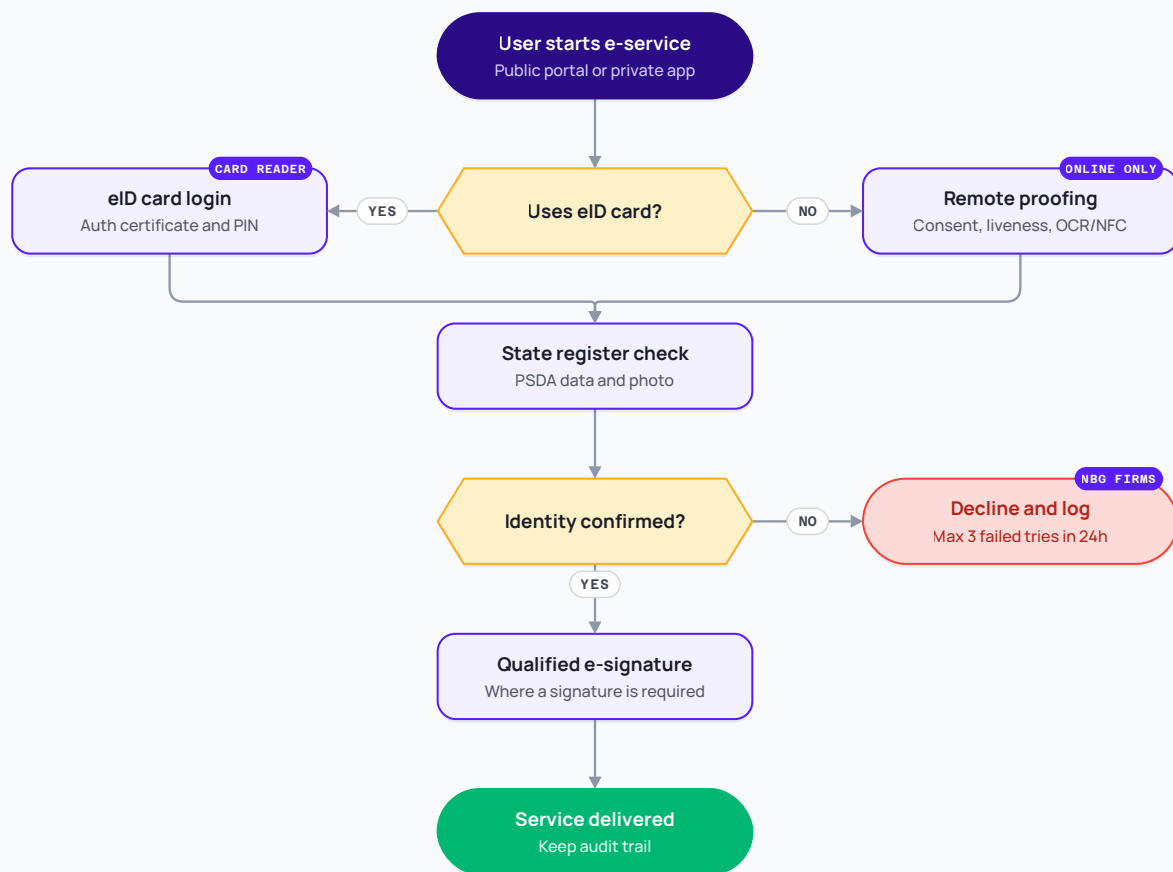


Figure 1. Remote identity proofing anchored on Georgia's state register.

Signing at the end of the flow

If a person or private entity chooses to communicate with an administrative body electronically and the document needs a signature or seal, a qualified electronic signature or seal is mandatory (Article 3(3)). Administrative bodies must themselves sign or seal electronic documents with a qualified signature or seal; a qualified seal alone suffices (Article 3(4)).

5

Digital channels: what's different

Bottom line: the legal basis for identity is channel-neutral, but online the signature requirement hardens into a qualified e-signature, and regulated firms proving identity remotely must add liveness and a register photo match that a counter visit does not need.

Requirement	In person / Public Service Hall	Online / remote	Difference
Proof of identity	Identity card, residence card or passport presented	eID authentication certificate, or remote proofing against PSDA data	Differs
Use of state register data	Permitted as proof of identity	Permitted as proof of identity	Same
Signing a filing to a public body	Handwritten signature	Qualified e-signature or seal mandatory	Differs
Non-resident filers	Handwritten signature	Exempt from the qualified-signature requirement	Differs
Passport application from abroad	Consulate or PSDA office	Electronic application if identifiable in the PSDA database	Differs
Liveness and face match (regulated firms)	Not required	Required, with PSDA photo or live document	Differs
Biometric data rules	Article 9 of the data protection law	Article 9 of the data protection law	Same
Breach notification	72 hours to the State Audit Office	72 hours to the State Audit Office	Same

Qualified signature becomes mandatory online

The requirement in Article 3(3) of the trust services law applies only when the person chooses the electronic channel. Since Law No. 2557-XIოლ-Xოჲ of 9 February 2023 it does not apply to non-residents, or where the law does not require a signature or seal at all. The Government may set further exemptions by legal act (Article 3(10)). For services open to foreign users, this means a lower-assurance electronic signature can be acceptable where the filer is a non-resident.

Remote applications for documents

Citizens abroad who already hold a Georgian passport or identity card, or who are registered, and who can be identified through the PSDA database, may apply for a passport

electronically under rules set by the Minister of Justice (Article 20²(7⁸) of the identity card law).

Stricter controls for regulated firms online

Under Order No. 104/04, a firm identifying a customer electronically must apply the same measures it would apply face to face. Face-matching software must reach a minimum accuracy of 1 in 10,000; video identification must be live, end-to-end encrypted, at least HD, and include at least three randomly chosen tasks, with no pre-recorded video. Each customer may make no more than three failed attempts in 24 hours, failed or interrupted attempts must be classified and kept for at least one year, and suspicious attempts must be blocked by personal number and other identifiers such as IP address.

6 Data protection and biometrics

The Law of Georgia on Personal Data Protection (No. 3144-XI⁰ლ-X⁰ჟ, 14 June 2023) applies to public and private controllers alike.

Biometrics as a special category

Biometric data, defined to include facial images, voice characteristics and fingerprints processed by technical means that allow unique identification, is special-category data when processed to identify a person uniquely (Article 3(b) and (d)). Processing it needs a ground under Article 6, such as the data subject's written consent or a specific legal provision that makes the processing necessary and proportionate. Article 9, in its current wording (amended by Law No. 1054 of 12 November 2025), allows biometric processing where necessary for carrying out an activity, security, property protection or preventing disclosure of secret information and where the aim cannot otherwise be achieved without disproportionate effort, as well as for issuing identity documents, identifying people at the border and other listed public purposes. Before processing starts, the controller must define in writing the purpose and scope, the retention period, the storage and destruction rules and the mechanisms protecting data subjects' rights.

Obligations that bite on identity systems

Every public institution must appoint a personal data protection officer and register the officer with the State Audit Office within 10 working days (Article 33). A data protection impact assessment is mandatory before processing special-category data of a large number of people, defined as at least 3 percent of the population, and before fully automated decisions with legal effect (Article 31). Incidents must be reported to the State

Audit Office within 72 hours of discovery unless unlikely to cause significant harm (Article 29). Controllers established outside Georgia that process data using technical means in Georgia must register a special representative first, unless established in the EU or in a country the EU recognises as adequate (Article 34). **In force**

7 Sector-specific obligations

Obligations of trust service providers

A qualified trust service provider must identify every person to whom it issues a certificate in line with the technical regulation, keep records of certificates and related data for at least six years after revocation, provide online certificate-status information continuously, and notify the DGA of any security breach within 24 hours (Articles 5 and 6 of the trust services law). A certificate that has been suspended for 10 calendar days without renewal is revoked.

Information security for public bodies

The Law of Georgia on Information Security applies to critical information system subjects. Amendments adopted on 10 June 2021 divided those subjects into three categories, defined the powers of the Operational-Technical Agency of the State Security Service and introduced administrative sanctions. The law was last amended on 26 June 2025. Public bodies classed as critical information system subjects carry these obligations into any identity system they operate.

Document issue and lifecycle

Identity and residence cards are issued by the PSDA through territorial offices and Public Service Halls, and abroad through consulates. A person may replace a card or passport when less than six months of validity remain (Articles 18(6) and 20⁵(10), added from 1 January 2026).

IDENTITY-ABUSE INDICATORS IN REMOTE PROOFING

- **Repeated failed attempts:** several failed sessions against one personal number or IP address.
- **Pre-recorded media:** a photo of a document or a recorded face instead of a live session.
- **Register mismatch:** document data that differs from the PSDA record, or a document reported lost or expired.
- **Interrupted sessions:** video calls that drop or cannot be completed without breaks.
- **Coached applicant:** behaviour suggesting the person is acting under someone else's influence.
- **Proxy use:** attempts to onboard electronically through a representative.
- **Anonymised location:** VPN, proxy or TOR use that hides where the applicant is.

These indicators are drawn from the termination and attempt-control rules of National Bank Order No. 104/04 (Articles 2, 4 and 6).

Data protection enforcement is the main exposure for identity systems. The State Audit Office can order breaches remedied, require processing or international transfers to stop, order data blocked, deleted or destroyed, and impose administrative liability (Article 52). Fines are fixed per offence and tiered by turnover: the lower tier covers natural persons, public institutions, non-commercial entities and businesses with annual turnover up to GEL 500,000, and the higher tier covers businesses above GEL 500,000. Under the amendments made by Law No. 1289 of 17 December 2025:

Offence	Lower tier	Higher tier
Failure to notify an incident (Article 78(1))	Warning or GEL 2,000	Warning or GEL 3,000

Failure to comply with a lawful State Audit Office requirement (Article 87)	Warning or GEL 1,000	Warning or GEL 2,000
Obstructing an inspection (Article 86(3))	Warning or GEL 2,000	Warning or GEL 4,000
Repeated failure to appoint a data protection officer within a year (Article 82(2))	GEL 3,000	
Repeated failure to appoint a special representative within a year (Article 83(2))	GEL 5,000	

Decisions can be appealed to court within one month. For trust services, the DGA's sanction is suspension or termination of authorisation, and the provider is liable in damages. For regulated firms, breach of Order No. 104/04 allows the National Bank to apply supervisory measures and sanctions, and a customer identified electronically in breach of the order is treated as unidentified.

10 Recent changes and what to watch

- **2 March 2026** **In force** The Personal Data Protection Service was liquidated and the State Audit Office became its successor; existing bylaws stay in force until the Auditor General replaces them.
- **1 January and 1 July 2026** **In force** New electronic identity card content took effect, including fingerprints, a QR code and an authentication certificate; temporary identification cards changed from 1 July 2026.
- **16 December 2025** **In force** National Bank Order No. 288/04 added a duty to assess sanctions evasion risk during electronic onboarding.
- **12 November 2025** **In force** Law No. 1054 rewrote the grounds for biometric processing in Article 9 of the data protection law.
- **23 June 2025** **In force** National Bank Order No. 142/04 required an independent audit opinion on outsourced onboarding providers' data deletion by 1 February 2026.
- **29 April 2025** **In force** National Bank Order No. 104/04 replaced the 2021 remote identification rule and gave existing users nine months to comply.

What this means for identity verification

For Georgian citizens and residents, the PSDA register is the anchor: build a register check and a comparison of the live face with the register photograph into every remote flow. Support the electronic identity card both as a document (read by NFC using the CAN) and, where available, as an authentication and signing credential. Expect cards issued from 2026 to carry fingerprints and a QR code, while older valid cards stay in circulation.

For non-residents, there is no register record, so document authenticity checks and, for regulated firms, an additional verification such as a transfer from an account in the customer's name, carry the weight. Treat any face template as special-category data: document the purpose, retention and deletion rules in writing before launch, run an impact assessment at scale, and keep failed-attempt logs for the period the applicable rules require. Where a filing to a public body is signed online, route the user to a qualified electronic signature unless a non-resident or no-signature exemption applies.

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 Georgian electronic ID cards and passports.
- Biometric liveness and face match against a live document or a registry photograph.
- Configurable attempt limits, decline logging and an audit trail for each verification session.
- Qualified-signature-ready e-signature steps at the end of an onboarding flow.
- Cloud, on-premises or hybrid deployment to fit public-sector data residency needs.

[Request a meeting](#)

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 დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ [Law of Georgia on Electronic Documents and Electronic Trust Services], No. 639-III, 21 April 2017, consolidated to 9 February 2023, Articles 1 to 14, matsne.gov.ge; English version matsne.gov.ge
- Law No. 6298-III of 12 June 2020 amending Article 11 of the trust services law, matsne.gov.ge
- საქართველოს მოქალაქეთა და საქართველოში მცხოვრებ უცხოელთა რეგისტრაციის, პირადობის (ბინადრობის) მოწმობისა და საქართველოს მოქალაქის პასპორტის გაცემის წესის შესახებ [Law on the Procedure for Registering Citizens and Aliens and Issuing Identity (Residence) Cards and Passports], No. 323, 27 June 1996, consolidated to 17 December 2025, matsne.gov.ge
- Law No. 1120-IVმს-XIშპ of 26 November 2025 amending the identity card law, in force 1 January 2026 (Article 14(11) and (12) from 1 July 2026), matsne.gov.ge
- Law of Georgia on the Legal Entity under Public Law called the Digital Governance Agency, No. 6297-III, 12 June 2020, Articles 2, 4, 6 and 10, matsne.gov.ge
- პერსონალურ მონაცემთა დაცვის შესახებ [Law of Georgia on Personal Data Protection], No. 3144-XIმს-Xშპ, 14 June 2023, consolidated to 10 June 2026, Articles 3 to 9, 29, 31, 33 and 34, matsne.gov.ge
- Law No. 1289-IVმს-XIშპ of 17 December 2025 amending the Law on Personal Data Protection (State Audit Office, Articles 49 to 87, transitional Article 2), matsne.gov.ge
- Law of Georgia on Information Security, No. 6391-III, 5 June 2012, list of amending acts to 26 June 2025, matsne.gov.ge
- Parliament of Georgia, "Parliament Endorsing Changes to Law on Information Security with III Reading", 10 June 2021, parliament.ge
- National Bank of Georgia, Order No. 104/04 of 29 April 2025, Rule on carrying out preventive measures electronically by an obliged entity, as amended by Orders No. 142/04 (23 June 2025) and No. 288/04 (16 December 2025), Articles 1 to 7, nbg.gov.ge
- Public Service Development Agency, "Electronic identity card", page revised 20 March 2025, sda.gov.ge