



Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in Georgia

COUNTRY Georgia

INDUSTRY Fintech & Digital Payments

LAST UPDATED 16 October 2026

KEY REGULATORS National Bank of Georgia · Financial Monitoring Service of Georgia · State Audit Office of Georgia

Key takeaways

- Only a company incorporated in Georgia can offer payment or e-money services, and it must first be registered by the National Bank of Georgia (NBG); banks, microbanks and NBG-registered microfinance organisations are exempt from separate registration.
 - Payment and e-money providers are fully covered by Georgia's anti-money laundering (AML) law: they must identify and verify every customer before opening a relationship, screen against sanctions lists and report suspicious transactions to the Financial Monitoring Service the same day.
 - App-only onboarding is allowed, but only after the NBG gives written consent to the provider's remote process, backed by an independent audit report; a selfie with liveness detection and a live document check are mandatory.
 - Remote onboarding is restricted for foreigners: nationals of high-risk jurisdictions cannot be onboarded online, and non-residents need extra verification such as a 1 tetri transfer from an account in their name or software that validates the document.
 - Customer money must be held in full in segregated accounts at a Georgian bank, and the NBG publishes fines per violation, including up to GEL 100,000 for repeated systemic AML failures.
-

Georgia is open to digital payment and e-money businesses, including app-only models, but through a single national route: registration with the National Bank of Georgia as a payment service provider. There is no regional licensing and no passporting from foreign licences; the applicant must be a Georgian legal entity with a head office and data backups in the country.

The NBG is both the licensing authority and the AML supervisor for payment providers, while the Financial Monitoring Service of Georgia receives suspicious transaction reports. Personal data protection, including biometric data, is supervised by the State Audit Office from 2 March 2026.

The biggest obstacle for a new entrant is usually the remote onboarding approval: the NBG must consent in writing to the electronic customer due diligence process before it goes live, and the rules on liveness, document checks, data location and outsourcing are prescriptive.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 AML, KYC and customer due diligence
- 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 for fintech and payments	Level	Official site
National Bank of Georgia	Registers and supervises payment service providers, e-money providers, microfinance organisations and currency exchange offices; AML supervisor for these entities; approves remote onboarding processes; runs the regulatory sandbox	National	nbg.gov.ge
Financial Monitoring Service of Georgia	Financial intelligence unit; sets identification data and reporting rules; receives suspicious and threshold reports; can order a 72-hour suspension of a transaction	National	fms.gov.ge
State Audit Office of Georgia	Personal data protection supervisor since 2 March 2026 (successor to the Personal Data Protection Service)	National	pdp.sao.ge
Public Service Development Agency	Holds the state identity database that obliged entities may query, without the customer's consent, to verify identity	National	sda.gov.ge
Government Commission on the implementation of UN Security Council resolutions	Designations and asset freezes under UN Security Council Resolution 1373	National	Legal basis on Matsne

Licensing and supervision are national. EU law does not apply directly in Georgia, even where Georgian rules follow EU models.

2 Licensing and authorisation

Registration as a payment service provider

Under NBG Order No. 77/04 of 1 May 2023, no one may provide payment services, including money remittance, unless registered by the NBG, and only a legal entity founded and registered under Georgian law may apply. Commercial banks, microbanks and NBG-registered microfinance organisations are outside this registration requirement. The same rule covers e-money issuers, which are payment service providers that issue electronic money. **In force**

The application includes a schematic of each payment service showing every flow of information and money, a demonstrable electronic system, a three-year business plan for activity in Georgia, ownership and beneficial owner documents, ten-year criminal record certificates and, where relevant, compliance plans for the NBG's strong customer authentication and wire transfer rules. The NBG decides within 60 calendar days of a complete file.

Substance requirements

Head office in Georgia

Administrators must manage the business from a physically separate head office in Georgia, and one authorised representative must be in Georgia at least 14 days a month.

Data in Georgia

Backups of each customer's balance records must be made at least daily and stored in a data centre in Georgia, retrievable from the head office.

Fit and proper

Administrators need relevant higher education or two years' managerial experience in finance; convictions for serious or economic crimes disqualify administrators and significant shareholders. A sole shareholder who is also director must appoint a second director.

Safeguarding

Customer funds must sit in nominee accounts at a Georgian commercial bank or microbank: 100% of e-money issued and of non-cash funds at the end of each banking day, or an NBG-approved bank guarantee.

A provider becomes a "significant" provider if its average monthly payment volume over 12 months exceeds GEL 9,000,000, or if an e-money provider's average daily outstanding e-money over six months exceeds GEL 1,500,000; significant providers must meet the NBG's capital adequacy rule and additional governance and outsourcing requirements. Payment initiation providers must also show minimum supervisory capital at registration.

Agents, outsourcing and the sandbox

A provider must notify the NBG 30 days before using agents and is fully liable for them, including for AML compliance. Outsourcing is barred to jurisdictions where the NBG could lose access to information. The NBG's regulatory sandbox (Order No. 125/04 of 23 May 2025) allows controlled live testing of new products.

The NBG may cancel a registration for, among other grounds, AML breaches, misleading documents or not starting services within three months; most cancellations bar the owners from reapplying for three years. Microfinance organisations, loan-issuing entities and currency exchange offices follow separate NBG registration regimes and are obliged entities in their own right; under an amendment adopted on 1 April 2026, factoring companies and factoring platforms join the list of AML obliged entities from 1 January 2027.

Adopted, effective 1 Jan 2027

3

AML, KYC and customer due diligence

Payment service providers, microfinance organisations, currency exchange offices, loan-issuing entities, microbanks and banks are all "obliged entities" (financial institutions) under Article 3 of the Law of Georgia on Facilitating the Prevention of Money Laundering and the Financing of Terrorism (No. 5226-lb, 2019), and the NBG is their supervisor under Article 4. For open banking, the law does not apply to account information services, and payment initiation requires only customer identification and verification.

When due diligence is required

Under Article 11, preventive measures (identification and verification of the customer and beneficial owner, the purpose of the relationship, and ongoing monitoring) apply when a business relationship is established; for an occasional transaction above GEL 15,000 (or linked transactions); for an occasional wire transfer above GEL 3,000; whenever there is doubt about identification data; and at any amount where money laundering or terrorist financing is suspected. Verification must be completed before the relationship starts, although for lower-risk customers it may finish afterwards if needed to avoid interrupting

service, as soon as reasonably possible. Anonymous accounts and accounts in fictitious names are prohibited.

Simplified and enhanced measures

Article 9 allows the Financial Monitoring Service, by its own normative act, to exempt low-value e-money instruments that can only pay for goods and services, cannot hold more than GEL 500 (up to GEL 1,500 if usable only in Georgia), cannot be loaded anonymously, and allow no more than GEL 150 in cash withdrawals. Enhanced measures apply to higher-risk customers (Article 18), politically exposed persons and their family and close associates (Article 21) and customers linked to high-risk jurisdictions on the NBS's list (Article 19); they include source of funds and wealth checks and management approval.

Beneficial ownership, reporting and records

- **Beneficial owner:** a natural person owning or controlling 25% or more of a legal entity, directly or indirectly, or otherwise exercising ultimate control (Article 13).
- **Suspicious transactions:** reported to the Financial Monitoring Service on the day reasonable suspicion arises (Article 26), including attempted transactions; tipping off is prohibited.
- **Information requests:** answered within two working days (Article 26).
- **Threshold reports:** further transaction types reportable to the Service are set by Financial Monitoring Service Order No. 1 of 5 June 2020, last amended on 17 November 2025.
- **Records:** kept for five years after the relationship ends or the occasional transaction, extendable by up to five years on request (Article 27).

Every obliged entity needs a compliance control system with a senior compliance officer, training and independent audit (Article 29), and must assess the risk of any new technology or channel before launch (Article 8).

4 Identity verification and onboarding

Financial Monitoring Service Order No. 2 of 5 June 2020 sets the identification data. For individuals this covers name, date and place of birth, personal number, document number, sex, citizenship and address. Accepted documents for Georgian citizens are a passport, identity card or driving licence; for foreign nationals a residence card, passport or another document accepted for crossing the Georgian border. The document must bear a photograph and be valid. For legal entities, a Georgian public registry extract or a foreign

registry extract dated within six months is required. Remote identification and beneficial owner verification follow the supervisor's own rules rather than this order.

Article 16 (7) of the AML law lets obliged entities and their outsourcers query the Public Service Development Agency's databases without the customer's consent. Reliance on a regulated third party is allowed, except one in a high-risk jurisdiction, and the obliged entity keeps ultimate responsibility.

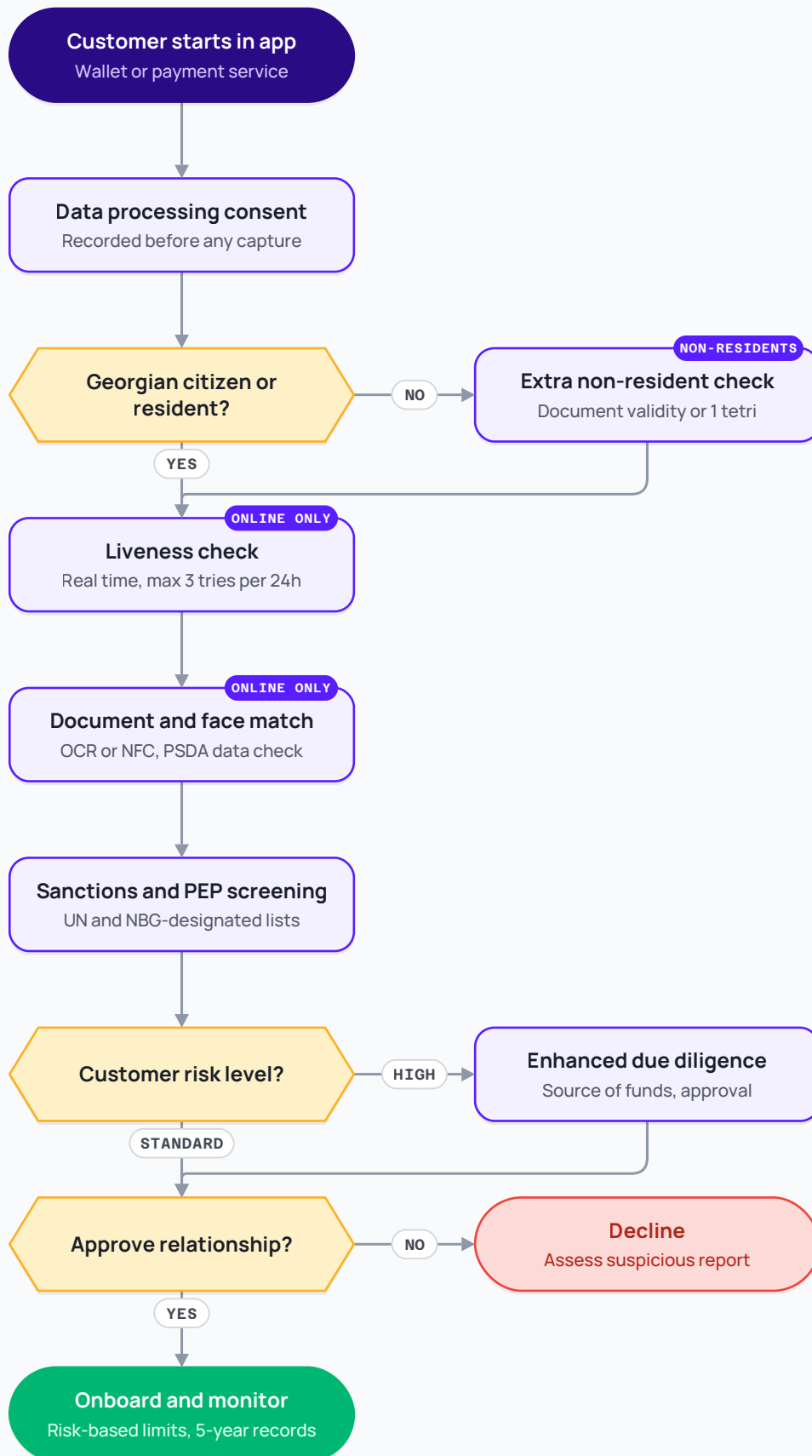


Figure 1. Remote onboarding of an individual by an NBG-supervised payment or e-money provider in Georgia.

NBG Order No. 104/04 of 29 April 2025 on carrying out preventive measures electronically governs how the steps in Figure 1 are performed for every NBG-supervised obliged entity. A customer onboarded in compliance with it counts as identified and verified; a customer onboarded in breach of it counts as unidentified. In force

5

Digital channels: what's different

Bottom line: Remote onboarding is permitted, but only through an NBG-approved process with mandatory liveness and live document checks, and it is closed to nationals of high-risk jurisdictions and to some foreign corporate customers who could be onboarded in person.

Requirement	In person	Online / remote	Difference
Permission to onboard	Under the AML law and Order No. 2	Only after NBG written consent to the process and an independent audit report	Differs
Due diligence content	Full preventive measures	The same measures as face to face, plus the same risk-based documents	Same
Biometrics	Not required	Real-time liveness check and face match against the document or state database photo	Differs
Document check	Original seen, copy certified by staff	Document held live on camera, data read by OCR or NFC, Georgian documents checked against the state database	Differs
Non-resident individuals	Passport or border-crossing document	Document validity software, a 1 tetri transfer from own account or another reliable method; high-risk nationals barred	Differs
Corporate customers	Any jurisdiction, with full due diligence	Only Georgian or listed-country entities and owners; paper documents within 60 days	Differs

Acting through a proxy	Allowed with notarised authority	Prohibited, with narrow exceptions for company directors	Differs
Sanctions and PEP screening	Required	Required before onboarding	Same
Evidence kept	Five years	Five years, plus failed attempts for at least one year and full video for agent-led sessions	Differs

Approval, data location and outsourcing

Before introducing or changing a remote process, the provider must apply to the NBG with the Annex 2 form and an independent auditor's report; the NBG decides within 30 calendar days, extendable by 30. The full information asset, including backups, must be kept only on the provider's side: an outsourced verification vendor may keep only a technical audit log, and the provider must have high assurance that the vendor deletes everything else. The provider must commission an annual independent information security audit and penetration test.

Technical standards for liveness and matching

The process must collect consent, run a liveness check and verify the document in real time. Liveness technology must be checked by a qualified third party; a 3D face scan is recommended where no human is involved. Automated face matching must achieve a minimum accuracy of 1 in 10,000, staff must sample automated decisions, and failed attempts are capped at three per customer in 24 hours. Agent-led video identification needs encrypted HD video, at least three randomly chosen tasks, the four-eyes principle and random allocation of staff; pre-recorded video is not allowed.

Foreign customers and high-risk jurisdictions

Under Order No. 288/04 of 16 December 2025, citizens or residents of a high-risk jurisdiction or offshore zone cannot be onboarded remotely unless they hold Georgian citizenship or residence. For remotely onboarded customers, international transfers linked to high-risk jurisdictions are prohibited, and the provider must detect card payments linked to them. For non-residents, the provider must document why the customer banks in Georgia and whether the account may serve for transit. **In force**

The Law of Georgia on Personal Data Protection (No. 3144, 2023) applies to all identity capture. From 1 May 2026, its rewritten Article 9(1) allows biometric data to be processed only where necessary for carrying out an activity, security, property protection or preventing disclosure of secret information, where these aims cannot be achieved otherwise without disproportionate effort, or in other cases expressly provided by law. For payment providers, the mandatory liveness and face-matching steps in NBG Order No. 104/04 are the clearest legal anchor, and that order requires consent to data processing as the first step of the remote process. **In force from 1 May 2026**

Since 2 March 2026 the State Audit Office supervises data protection: data breaches must be notified to it within 72 hours unless significant harm is unlikely, and a controller registered abroad that processes data using technical means in Georgia must appoint a special representative there. Under Order No. 104/04, transfers to a vendor in a country without adequate protection need security safeguards, contractual confidentiality and full information to the customer.

Wire transfer information

The payer's provider must ensure transfers carry the payer and payee information the NBG specifies (Article 17 of the AML law); a recipient or intermediary provider must assess whether missing information calls for a suspicious transaction report. Registration requires a compliance plan for the NBG's wire transfer information regulation (Order No. 253/04 of 30 November 2018).

Sanctions

Any person must freeze, without notice, funds of persons designated under UN Security Council resolutions and inform the Financial Monitoring Service; since an amendment of 26 November 2025, failure by persons outside the obliged-entity list is an administrative offence. NBG-supervised entities must also screen against the lists set by NBG Order No. 208/04 of 4 August 2023 on sanctions regimes, and Order No. 104/04 requires them to assess the risk of sanctions evasion in remote onboarding.

Complaints and data disclosure

Complaint records must be kept for at least six years. From 2 March 2026, the payment law lists who may receive a customer’s payment data, including the Financial Monitoring Service and the State Audit Office; anyone else needs a court decision.

8 Risk indicators and red flags

PAYMENT AND E-MONEY RED FLAGS DRAWN FROM NBS AND AML RULES

- **Transit use by non-residents:** a foreign customer with no clear reason to bank in Georgia or signs of pass-through flows.
- **Structuring:** linked occasional transactions or transfers kept just under GEL 15,000 or GEL 3,000.
- **High-risk corridors:** card payments or transfers involving high-risk jurisdictions or offshore zones by remotely onboarded customers.
- **Repeated failed e-ID attempts:** several failed sessions linked by personal number or IP address.
- **Coached or coerced applicants:** behaviour in video identification suggesting phishing or another person’s influence.
- **Proxy onboarding:** attempts to open an account remotely on someone else’s behalf.
- **Unlicensed counterparties:** corporate customers that are foreign online casinos, unregulated financial or virtual asset businesses.
- **Unexplained wealth:** activity inconsistent with the customer’s stated source of funds or business.

9 Enforcement and penalties

The NBS fines payment service providers under Order No. 87/04 of 13 June 2017 (amended most recently on 1 May 2025). AML breaches are tiered and fined per violation, per customer or per day:

Tier	Examples	Fine (GEL)
------	----------	------------

Especially serious	Failing to file a suspicious transaction report on time; ignoring a suspension order; no screening system or a seriously defective one; anonymous accounts	5,000 to 15,000 per case
Serious	Serving a customer without identification or beneficial owner checks (1,000 each); no risk rating or no source of funds review (3,000 per customer); PEP failures (5,000 per person)	1,000 to 7,000
Less serious	Late threshold reports; record-keeping and wire transfer data failures	100 to 2,000
Systematic and systemic	Repeated breaches after a prior fine; breaches creating systemic risk	Up to 20,000 per case; up to 100,000

Payment-law breaches carry separate fines, such as 1% per day of any safeguarding shortfall (at least GEL 300). In a published decision, the NBG fined e-money provider eMoney Georgia JSC GEL 93,000, mainly for failing to establish the source of wealth and funds of 19 customers, ignoring risk factors in customer risk ratings and not filing suspicious transaction reports.

10 Recent changes and what to watch

- **1 January 2027:** **Adopted, effective 1 Jan 2027** Factoring companies and factoring platforms become AML obliged entities under the NBG, adding a new class of lenders and platforms to the regime.
- **1 May 2026:** **In force** New Article 9(1) of the data protection law narrows when biometric data may be processed; firms should document the legal basis for selfie and liveness checks.
- **2 March 2026:** **In force** The State Audit Office replaced the Personal Data Protection Service as supervisor; breach notifications and special representative registrations go to it.
- **2 March 2026:** **In force** Amended Article 43(2) of the payment law lists who may receive customer payment data without a court decision.
- **1 February 2026:** **Deadline passed** Providers using outsourced remote verification had to evidence vendor-side storage and deletion controls with an independent audit report.

- **16 December 2025:** **In force** NBG Order No. 288/04 tightened remote onboarding of non-residents and transfers linked to high-risk jurisdictions.
- **26 November 2025:** **In force** AML law amendment strengthened UN sanctions freezing and created administrative liability for non-compliance by any person.

11 What this means for identity verification

For a Georgian payment or e-money app, the remote flow is effectively specified by regulation: recorded consent, a real-time liveness check with a fresh photo, a live document capture read by OCR or NFC with security feature checks, and comparison with the Public Service Development Agency database for Georgian documents. Face matching must meet the 1 in 10,000 accuracy floor and be sampled by staff. Build attempt counters, suspicious-attempt logging by personal number and IP address, and one-year retention of failed sessions into the product.

Non-resident journeys need a separate branch: document validity software or a 1 tetri reference transfer, nationality and residence screening against high-risk and offshore lists, and a written rationale. Online corporate onboarding is limited to Georgian or listed-country structures, with paper documents within 60 days. Verification data and backups must sit with the provider, not the vendor, and a change of software supplier needs renewed NBG agreement.

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 KYC onboarding with ID document capture and verification, including NFC reading, to support live document checks.
- Biometric liveness detection and face match for the real-time checks required in remote onboarding.
- Video KYC for agent-led video identification sessions.
- AML screening against sanctions and PEP lists at onboarding and through ongoing monitoring.
- Cloud, on-premises or hybrid deployment to keep verification data on the provider's side.

[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

- ფულის გათეთრებისა და ტერორიზმის დაფინანსების აღკვეთის ხელშეწყობის შესახებ [Law of Georgia on Facilitating the Prevention of Money Laundering and the Financing of Terrorism], No. 5226-1b, 30 October 2019, consolidated version of 1 April 2026, Arts 2, 3, 4, 8 to 13, 16 to 21, 24 to 29, 41, Matsne, matsne.gov.ge
- NBG Order No. 104/04, 29 April 2025, Rule on carrying out preventive measures electronically by an obliged entity (consolidated with Orders No. 142/04 and No. 288/04), National Bank of Georgia, nbg.gov.ge
- NBG Order No. 288/04, 16 December 2025, amending Order No. 104/04, Matsne, matsne.gov.ge

- NBG Order No. 77/04, 1 May 2023, Rule on registration and regulation of payment service providers, Arts 1 to 17, Matsne, matsne.gov.ge; amending Order No. 48/04, 27 February 2025, matsne.gov.ge
- NBG Order No. 87/04, 13 June 2017, Rule on fines for payment service providers and their administrators (as amended to Order No. 111/04, 1 May 2025), Arts 2, 2¹, 2², National Bank of Georgia, nbg.gov.ge
- Financial Monitoring Service Order No. 2, 5 June 2020, Rule on identification and verification of a customer by an obliged entity, Arts 1, 4 to 7, 12, 13, 16, 17, Matsne, matsne.gov.ge; amending Order No. 1, 29 October 2025, matsne.gov.ge
- Financial Monitoring Service Order No. 2, 17 November 2025, amending Order No. 1 of 5 June 2020 on recording, storing and submitting transaction information, Matsne, matsne.gov.ge
- Law No. 1303-IV^{აბს-ქიშპ}, 17 December 2025, amending the Law on Payment System and Payment Services (Art 43(2)), in force 2 March 2026, Matsne, matsne.gov.ge
- Law No. 1259-IV^{აბს-ქიშპ}, 17 December 2025, amending the Law on Personal Data Protection (Art 9(1)), in force 1 May 2026, Matsne, matsne.gov.ge
- Law No. 1289-IV^{აბს-ქიშპ}, 17 December 2025, amending the Law on Personal Data Protection (transfer of supervision to the State Audit Office, Arts 29, 34), Art 1 in force 2 March 2026, Matsne, matsne.gov.ge
- Regulatory Laboratory (Order No. 125/04, 23 May 2025), National Bank of Georgia, nbg.gov.ge
- The monetary fine was imposed on payment service provider "eMoney Georgia" JSC, National Bank of Georgia AML/CFT supervision, nbg.gov.ge