



Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Georgia

COUNTRY Georgia

INDUSTRY Banking & Digital Banking

LAST UPDATED 16 October 2026

KEY REGULATORS National Bank of Georgia · Financial Monitoring Service of Georgia

Key takeaways

- Taking deposits and lending them out in your own name requires a banking licence from the National Bank of Georgia. A conditional licence with temporarily relaxed capital rules exists for innovative, technology-led entrants.
- Banks may onboard customers fully online, but only after the National Bank gives written consent to the remote process, supported by an independent audit. Customers onboarded through a non-compliant process count as unverified.
- Every remote onboarding must include a liveness check, a real-time check that the identity document is genuine, and a face match. Georgian citizens and residents are also checked against the state identity database.
- Non-residents can be onboarded online with extra checks, but nationals and residents of high-risk jurisdictions cannot. Foreign companies qualify only if they and all their owners come from the listed countries.
- Banks report suspicious activity to the Financial Monitoring Service on the day suspicion arises, and report large cash and high-risk transfers within five working days. Factoring companies join the regime on 1 January 2027.

Georgia is open to digital banking. The country has one national licensing regime, run by the National Bank of Georgia, which also supervises banks for anti-money laundering compliance. The Financial Monitoring Service of Georgia receives and analyses reports.

The biggest obstacle for a new entrant is the licence itself: capital, fit-and-proper owners and managers, and a head office in Georgia. For an app-first bank, the second obstacle is getting the National Bank's approval for its remote onboarding process, which follows a detailed technical rulebook.

CONTENTS

- | | |
|--|--|
| 1 Who regulates this sector | 7 Sector-specific obligations |
| 2 Licensing and authorisation | 8 Risk indicators and red flags |
| 3 AML, KYC and customer due diligence | 9 Enforcement and penalties |
| 4 Identity verification and onboarding | 10 Recent changes and what to watch |
| 5 Digital channels: what's different | 11 What this means for identity verification |
| 6 Data protection and biometrics | ▪ Sources |

1

Who regulates this sector

Authority	Remit	Level	Official site
National Bank of Georgia	Bank licensing, prudential supervision, AML/CFT supervision, approval of remote onboarding, sanctions compliance rules	National	nbg.gov.ge
Financial Monitoring Service of Georgia	Financial intelligence unit: suspicious and threshold reports, identification rules for all obliged entities	National	fms.gov.ge
Public Service Development Agency (Ministry of Justice)	State identity database that banks may query to verify individuals	National	sda.gov.ge
National Agency of Public Registry (Ministry of Justice)	Register of entrepreneurs used to verify Georgian companies and trace ownership	National	napr.gov.ge
State Audit Office of Georgia	Personal data protection supervisor since 2 March 2026	National	pdp.sao.ge

Georgia is a unitary state, so licensing and supervision are national.

2

Licensing and authorisation

Under Article 2 of the Law of Georgia on Commercial Bank Activities, no one may attract deposits and use them to issue loans in their own name without a National Bank licence. The word "bank" is also reserved for licensed banks and microbanks. A commercial bank must be a joint stock company.

Licensing conditions

Article 3 lists the conditions. Paid-up capital must meet the National Bank's minimum. Administrators and significant shareholders must pass fit-and-proper tests. The group, ownership and governance structure must be transparent and supervisable. The business plan must be viable. The head office, where most management decisions are taken, must be in Georgia.

The application under Article 3¹ must map every ownership level up to significant beneficial owners, with criminal record certificates covering the last 10 years and the source of their funds.

Conditional licence for innovative entrants

Article 3(2) allows the National Bank to issue a conditional licence with temporarily simplified minimum capital requirements. The National Bank sets restrictions and a staged timetable for meeting the full requirements.

Timeline

Under Article 4, the National Bank checks completeness within 5 working days and gives up to 15 working days to fix gaps. It reviews a complete application within 6 months, with the clock paused while it waits for extra information. The whole decision may not exceed 12 months. Licences are indefinite and cannot be transferred. Payment and microbank licences are separate regimes.

3

AML, KYC and customer due diligence

Commercial banks are obliged entities under Article 3(1) of the Law of Georgia on Facilitating the Prevention of Money Laundering and the Financing of Terrorism (No. 5226-Ilb, 2019), and the National Bank is their supervisor under Article 4. **In force**

When due diligence applies

Article 10 requires four measures:

- identifying the customer and verifying them from a reliable, independent source;
- identifying the beneficial owner and taking reasonable steps to verify them;
- establishing the purpose and intended nature of the relationship;
- monitoring the relationship.

Article 11 applies these measures in four situations:

- opening any business relationship;
- an occasional transaction above GEL 15,000;
- a one-off funds transfer above GEL 3,000;
- whenever the bank doubts identification data it already holds.

Suspicion triggers the full measures regardless of amount.

Timing and refusal

Article 12 requires due diligence before the relationship starts. For lower-risk customers, verification may be completed afterwards if needed to avoid interrupting service. An account may be opened before verification, provided no operations are allowed on it until verification is complete. Anonymous and fictitious-name accounts are banned. If due diligence cannot be completed, Article 10(6) prohibits starting or continuing the relationship and requires the bank to consider a suspicious transaction report.

Enhanced and simplified measures

Article 18 sets enhanced measures for higher-risk customers:

- additional information on the customer's property and activity;
- more frequent updates of customer data;
- management approval for the relationship;
- reasonable steps to establish the source of funds;
- enhanced monitoring.

Article 21 applies management approval, source-of-wealth checks and enhanced monitoring to politically exposed persons (PEPs), their family members and close associates, and requires continuing risk management after a PEP leaves office.

Article 19 requires enhanced measures for customers linked to high-risk jurisdictions, on a list the National Bank approves on the Financial Monitoring Service's proposal. Georgian citizens and residence permit holders are exempt from the residence-based trigger. Simplified measures under Article 24 are allowed only where risk is lower and never where higher-risk indicators exist.

Beneficial ownership

Under Article 13, a beneficial owner of a legal entity holds 25 per cent or more of the shares or voting rights, directly or indirectly, or otherwise exercises ultimate control. If none can be found, senior managing officials are treated as beneficial owners. National Bank Order No. 189/04 (2020) sets how ownership structures are examined and beneficial owners verified.

Reporting and record keeping

Suspicious transaction reports are due on the day reasonable suspicion arises (Article 26(2)), regardless of amount. The bank must also report the transactions in the table below to the Financial Monitoring Service within 5 working days (Order No. 1 of the Head of the Financial Monitoring Service, Articles 5 and 9; version of 17 November 2025).

Transaction (commercial banks)	Report if above
Cash deposit to an individual's account	GEL 50,000
Cash deposit to a legal entity's account	GEL 100,000
Cash purchase or sale of foreign currency	GEL 50,000
Transfer to or from a high-risk jurisdiction	GEL 50,000
Transfer to or from a "suspicious zone" (weak AML controls, per the bank's own information)	GEL 300,000
Money remittance to or from a high-risk jurisdiction or suspicious zone	GEL 10,000
Foreign funds credited to a non-profit (not a charity)	GEL 50,000
Foreign funds credited to a charity	GEL 10,000

Article 27 requires customer and transaction records to be kept for 5 years after the relationship ends or the transaction is made. The Financial Monitoring Service or the supervisor may extend this by up to 5 years. Article 29 requires a compliance officer at senior management level and a board-level owner of the compliance system.

4

Identity verification and onboarding

Order No. 2 of the Head of the Financial Monitoring Service (5 June 2020) sets the identification data and documents for all obliged entities.

- **Data for individuals (Article 4):** full name, date of birth, personal number (if any), document number, sex, citizenship, place of birth, and actual and registered address.
- **Documents for Georgian citizens (Article 5):** passport, identity card or driving licence.
- **Documents for foreign nationals (Article 5):** residence card, passport or another document accepted for crossing the Georgian border.

Documents must be valid and carry a photograph. Banks may query the Public Service Development Agency's database without the person's consent, and the data must come with the person's photograph (Article 5(4); AML law Article 16(7)).

Georgian companies are verified with an extract from the National Agency of Public Registry. Foreign companies are verified with a registry extract or registration document dated no more than 6 months before verification (Article 7).

Third-party reliance

Article 16 of the AML law allows reliance on a regulated third party that applies Financial Action Task Force (FATF) standards. The bank must obtain the identification data immediately. Reliance on intermediaries in high-risk jurisdictions is prohibited. Agents and outsourced providers working under written contract are not third parties. Either way, the bank keeps final responsibility.

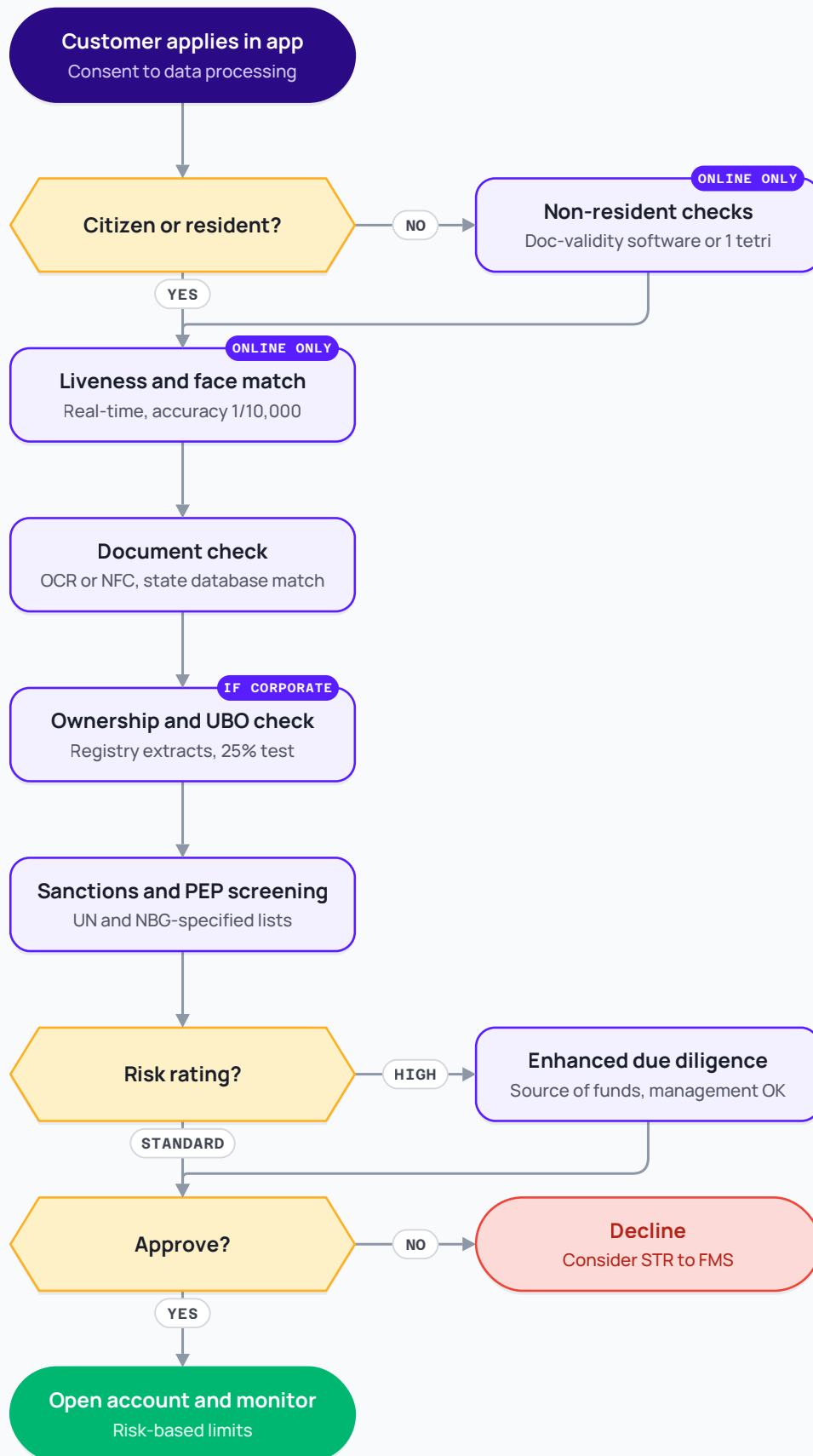


Figure 1. Remote retail and business onboarding at a Georgian bank under National Bank Order No. 104/04.

Bottom line: The due diligence content is the same online and in a branch. Remote onboarding, however, needs prior National Bank consent and must follow a prescribed technical standard (Order No. 104/04 of 29 April 2025). Customers onboarded through a non-compliant process are treated as unverified.

Requirement	In person	Online / remote	Difference
Permission to onboard	No separate approval	Prior written National Bank consent and independent audit report	Differs
Due diligence measures	AML law and Order No. 2	Same measures, same documents	Same
Biometrics	Photo document checked against the person	Liveness, real-time document check and face match	Differs
Document data capture	Not prescribed	Automatic reading by OCR or NFC	Differs
Failed attempts	Not prescribed	Maximum 3 failed attempts per 24 hours	Differs
Non-resident individuals	Passport or border document	Plus document-validity software or a transfer from own account; high-risk nationals excluded	Differs
Legal entities	Any jurisdiction, risk-based	Georgia or Annex 1 countries only; originals within 60 days	Differs
Sanctions and PEP screening	Required	Required	Same
Evidence kept	Records for 5 years	Plus full video; failed attempts kept at least 1 year	Differs

Approval before launch

Article 3 of Order No. 104/04 requires a written application with a completed Annex 2 form and an independent auditor's opinion, before launch and before any change. The National Bank decides within 30 calendar days, extendable by 30. It may require changes or suspend the process.

Annual independent information-security audits and penetration tests are mandatory.

The technical standard

Article 4 requires three steps: consent, a liveness check, and a real-time check that the document is genuine with comparison of the person to the document or to the state database photograph. The person must hold the physical document during the session; previously captured images are not accepted.

For Georgian identity documents and residence permits, the data must be fully matched against the Public Service Development Agency record. Automated face matching must reach a minimum accuracy of 1 in 10,000. Where staff take decisions, the four-eyes principle applies.

Video identification needs an encrypted, uninterrupted HD connection, at least three randomly chosen tasks, random assignment of the reviewing employee, and no pre-recorded video.

Non-residents, companies and limits

Non-resident individuals must be verified with software that can establish document validity, or a transfer of at least 1 tetri from another account in their name. That transfer may not come from a high-risk jurisdiction or offshore zone; EU and Schengen members are exempt from the offshore exclusion. Video identification of non-residents requires the transfer as well.

Remote onboarding is prohibited in these cases:

- nationals or residents of high-risk jurisdictions and offshore zones, unless they hold Georgian citizenship or residence;
- onboarding through a representative acting under power of attorney, with narrow exceptions for company directors;
- certain non-resident companies, including online casinos and unregulated financial or virtual asset firms.

Remotely onboarded customers may not make international transfers linked to high-risk jurisdictions or offshore zones. The bank must set risk-based limits on their transactions.

Outsourcing and data location

All data, logs and backups must be held only on the bank's side. An outsourced provider may keep only a technical audit log, and the bank must have high assurance that everything else is deleted.

6 Data protection and biometrics

The Law of Georgia on Personal Data Protection (No. 3144-XIმს-Xმპ, 2023) governs identity capture. Since 2 March 2026 it has been supervised by the State Audit Office, which took over from the former Personal Data Protection Service.

Article 9(1), rewritten with effect from 1 May 2026, allows biometric processing only in limited cases. One is where it is needed for carrying out an activity, security, property protection or preventing disclosure of secret information, and the aim cannot otherwise be achieved without disproportionate effort. Others include specified public purposes and cases directly provided by law. Article 9(2) requires the bank to define in writing, before processing, the purpose, scope, retention period, storage and destruction rules, and safeguards for data subjects.

Order No. 104/04 makes consent to data processing the first step of every remote session, while the AML law allows state database checks without consent. Data for an outsourced service may go to a country without adequate protection only with security safeguards, contractual confidentiality and full information to the customer.

7 Sector-specific obligations

Sanctions regimes

UN Security Council listings take direct effect in Georgia from publication on the UN committee's website (AML law, Article 41). Banks must screen customers, beneficial owners and payment counterparties before onboarding and as lists change (Order No. 1, Article 4).

National Bank Order No. 208/04 (4 August 2023) requires supervised entities to comply with US, EU and UK sanctions imposed on Russia and Belarus over the events in Ukraine. Banks may not deliver cash dollars, sterling or euros to foreign institutions or cash carriers except for transport to the US, the UK or the euro area. Monthly reports to the National Bank are due by the 20th or 25th of the following month.

An amendment of 19 September 2023 (Order No. 253/04) applies these regimes to Georgian citizens, and to Georgian companies they own, only where a Georgian court has issued a final guilty verdict on the grounds for the sanctions.

Correspondent banking

Before an international correspondent relationship, Article 22 requires the bank to assess the respondent's reputation, supervision and controls, obtain management approval, and document both sides' responsibilities. Relationships with shell banks and payable-through accounts are prohibited.

Tax status and account access

Article 21¹ of the Law on Commercial Bank Activities requires banks to determine customers' tax residence under the FATCA agreement with the United States and the Common Reporting Standard, and lets them refuse or close accounts if the customer withholds it. Banks may otherwise refuse service without reasons, except for the account defined in Article 20² of the Law on Payment Systems and Payment Services.

8

Risk indicators and red flags

BANKING INDICATORS DRAWN FROM GEORGIAN RULES AND ENFORCEMENT

- **Structuring:** transactions split to stay under reporting limits, which banks must actively detect (Order No. 1, Article 3(10)).
- **Transit accounts:** non-residents opening Georgian accounts with no clear local reason, which banks must analyse in writing.
- **High-risk corridors:** transfers or remittances to or from high-risk jurisdictions or weak-control zones.
- **Russia and Belarus flows:** remittances from these countries, monitored monthly under the sanctions rules.
- **Coerced applicants:** video sessions where the customer seems to act under someone else's direction.
- **Evasive onboarding:** vague answers, failed liveness tasks or poor-quality images, which require the bank to stop the process.

Enforcement and penalties

Article 30 of the Law on Commercial Bank Activities lets the National Bank act against a bank, its administrators or controlling persons for breaching the AML law, among other grounds. Its powers range from warnings and orders to fix controls, through limits on operations, dividends or deposit-taking and suspension of administrators, to monetary fines.

Fine amounts are set by a National Bank regulation on fines for commercial banks and their administrators. Published decisions count breaches per violation and per customer; late threshold reports, for example, are counted case by case in bands by length of delay.

In February 2026 the National Bank fined TBC Bank [GEL 250,000](#). The breaches were late and missed suspicious transaction reports, 23 customers without risk-appropriate measures, an outdated KYC file, unmet inspection requirements, and 66 late threshold reports. In August 2026 Terabank was fined [GEL 5,000](#) for failing to monitor one customer and examine the origin of their funds.

For remote onboarding, the larger risk is Article 1(6) of Order No. 104/04: every customer onboarded in breach of the rule is treated as unverified.

Recent changes and what to watch

- **1 January 2027** Adopted, effective 1 Jan 2027 Factoring companies and factoring platforms become obliged entities supervised by the National Bank (Law No. 1460-V^ალ-XI^მ of 1 April 2026).
- **1 May 2026** In force Article 9(1) of the data protection law rewritten, narrowing the grounds for biometric processing (Law No. 1259-IV^ალ-XI^მ). Biometric checks need a documented legal basis.
- **2 March 2026** In force Data protection supervision transferred to the State Audit Office (Law No. 1289-IV^ალ-XI^მ).
- **28 November 2025** In force AML law amended (Law No. 1119-IV^ალ-XI^მ): every person must freeze UN-listed assets, and suspicious transaction reports must state which assets were restricted.
- **29 April 2025** In force Order No. 104/04 replaced the 2021 remote onboarding rule, with a nine-month transition for approved banks.

What this means for identity verification

- **Before launch:** treat the remote onboarding stack as a regulated system. Plan for an independent audit, a National Bank decision window of up to 60 days, and re-approval whenever the vendor or process changes.
- **For Georgian customers:** combine real-time document capture (OCR or NFC) with liveness and a face match against both the document and the state database photograph.
- **For non-residents:** add document-validity checks or a micro-transfer from an own-name account, and screen nationality and residence against high-risk and offshore lists before the session starts.
- **For business customers:** confirm eligible jurisdictions for the company, every intermediate owner and every beneficial owner. Restrict the account until originals arrive within 60 days.
- **Data retention:** keep KYC data, liveness results and full video on bank-controlled infrastructure for at least 5 years, and failed sessions for at least 1 year. Cap retries at three per 24 hours.

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 onboarding with real-time ID document capture, including NFC chip reading, biometric liveness and face match.
- Video KYC sessions with randomised tasks and full session recording for the evidence trail.
- KYB and beneficial owner verification for business customers, including multi-level ownership structures.
- Screening against sanctions and PEP lists at onboarding and ongoing monitoring as lists change.
- On-premises or hybrid deployment where customer data and logs must stay on the bank's own infrastructure.

[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

- საქართველოს კანონი 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-III, 30 October 2019, consolidated version of 1 April 2026, matsne.gov.ge
- Law No. 1460-VIII-XI of 1 April 2026 amending the AML law (factoring, from 1 January 2027), matsne.gov.ge
- Law No. 1119-IVIII-XI of 26 November 2025 amending the AML law (sanctions and administrative liability), matsne.gov.ge

- **საქართველოს კანონი კომერციული ბანკების საქმიანობის შესახებ** [Law of Georgia on Commercial Bank Activities], No. 121, 23 February 1996, Articles 2, 3, 3¹, 4, 9, 21¹, 30, matsne.gov.ge
- **National Bank of Georgia, Order No. 104/04**, 29 April 2025, Rule on carrying out preventive measures electronically by an obliged entity, matsne.gov.ge
- **National Bank of Georgia, Order No. 189/04**, 21 October 2020, Rule on studying ownership and control structure and identifying and verifying the beneficial owner, matsne.gov.ge
- **National Bank of Georgia, Order No. 208/04**, 4 August 2023, Rule on compliance with sanctions regimes, matsne.gov.ge; amended by **Order No. 253/04**, 19 September 2023, matsne.gov.ge
- **Financial Monitoring Service of Georgia, Order No. 1**, 5 June 2020, Rule on recording, storing and submitting transaction information (version of 17 November 2025), Articles 3, 4, 5, 9, matsne.gov.ge
- **Financial Monitoring Service of Georgia, Order No. 2**, 5 June 2020, Rule on identification and verification of a customer, Articles 4 to 7, matsne.gov.ge
- **საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ** [Law of Georgia on Personal Data Protection], No. 3144-XIმს-Xმპ, 14 June 2023, Article 9, matsne.gov.ge
- **Law No. 1259-IVმს-XIმპ of 17 December 2025** (biometric data, in force 1 May 2026), matsne.gov.ge
- **Law No. 1289-IVმს-XIმპ of 17 December 2025** (transfer of data protection supervision, Article 1 in force 2 March 2026), matsne.gov.ge
- **National Bank of Georgia, Imposition of a Monetary Fine on JSC TBC Bank**, 3 February 2026, nbg.gov.ge
- **National Bank of Georgia, Imposition of a Monetary Fine on JSC Terabank**, 10 August 2026, nbg.gov.ge