

JSC “Neo Georgian Bank”
Personal Data Processing Policy

Table of Contents

1.	<i>General Provisions</i>	2
1.1.	<i>Purpose and Scope</i>	2
1.2.	<i>Who We Are</i>	2
1.3.	<i>Applicable Legislation</i>	2
1.4.	<i>Key Terms</i>	2
2.	<i>Categories of Personal Data</i>	3
2.1.	<i>Data Groups</i>	3
2.2.	<i>Various Cases of Data Processing</i>	4
3.	<i>Purposes, Grounds, and Retention Periods of Processing</i>	5
3.1.	<i>Legal Grounds</i>	5
3.2.	<i>Data Processing Table</i>	6
3.3.	<i>Direct Marketing</i>	7
3.4.	<i>Automated Decision-Making (Profiling)</i>	7
4.	<i>Sharing Data with Third Parties</i>	8
4.1.	<i>Grounds for Sharing</i>	8
4.2.	<i>Categories of Recipients</i>	8
4.3.	<i>International Transfer of Data</i>	9
5.	<i>Rights of the Data Subject</i>	10
5.1.	<i>List of Rights</i>	10
5.2.	<i>Exercising Rights</i>	11
6.	<i>Digital Channels and Cookies</i>	12
6.1.	<i>Online Banking / Mobile Banking</i>	12
6.2.	<i>Cookies Policy</i>	12
7.	<i>Data Retention Periods</i>	12
8.	<i>Information Security</i>	12
9.	<i>Communication and Complaints</i>	13

1. General Provisions

1.1. Purpose and Scope

This Personal Data Processing Policy (hereinafter – the Policy) defines the Bank’s approach to the processing of personal data. The document establishes what types of personal data the Bank processes, for what purposes, by what means, on what legal grounds, for how long it retains such data, and with whom it shares it.

The Policy applies to all of the Bank’s clients, including prospective clients, clients in pre-contractual relations, beneficial owners, borrowers, guarantors, owners of collateral, all customers and partners, and any person whose data the Bank processes.

1.2. Who We Are

JSC “Neo Georgian Bank” is a commercial bank licensed in accordance with the legislation of Georgia. For the purposes of this Policy, the Bank acts as the controller of personal data.

Bank identification code: 404785372

Legal address: 138a, David Aghmashenebeli Avenue, Tbilisi, Georgia]

Website: www.ngbank.ge

Email: privacy@ngbank.ge

1.3. Applicable Legislation

The Bank processes personal data in accordance with, among others, the following regulatory acts:

- The Law of Georgia “On Personal Data Protection”;
- The Law of Georgia “On Activities of Commercial Banks”
- The Law of Georgia “On Facilitating the Prevention of Money Laundering and Financing of Terrorism”
- The Law of Georgia “On Payment System and Payment Services”
- Regulatory acts of the National Bank of Georgia
- The European Union General Data Protection Regulation (GDPR).

1.4. Key Terms

The terms used in the Policy have the following meanings:

- 1.4.1. **Personal data** – any information relating to an identified or identifiable natural person. A natural person is identifiable when it is possible to identify them, directly or indirectly, including by name, surname, identification number, geolocation data, electronic communication identification data, or physical, physiological, mental, psychological, genetic, economic, cultural, or social characteristics;
- 1.4.2. **Data subject** – a natural person whose data the Bank processes.
- 1.4.3. **Processing** – any operation performed on data, including its collection, obtaining, access to it, photographing, video monitoring and/or audio monitoring, organization, grouping, interlinking, storage, alteration, retrieval, recall, use, blocking, erasure, or destruction, as well as disclosure of data by way of its transfer, publication, dissemination, or otherwise making it accessible;

- 1.4.4. **Special category data** – data relating to a natural person’s racial or ethnic origin, political opinions, religious, philosophical, or other beliefs, membership in a professional union, health, sex life, the status of an accused, convicted, acquitted, or aggrieved person in criminal proceedings, conviction, criminal record, diversion, recognition as a victim of trafficking in persons or, under the Law of Georgia “On Combating Violence against Women and/or Domestic Violence, Protection of and Support to Victims of Violence,” recognition as a victim of a crime, detention and the enforcement of a sentence against the person, as well as biometric and genetic data processed for the purpose of uniquely identifying a natural person;
- 1.4.5. **Data controller** – the Bank, which independently determines the purposes and means of data processing.
- 1.4.6. **Biometric data** – data processed using technical means, relating to the physical, physiological, or behavioral characteristics of a data subject (such as, for example, facial image, voice characteristics, or fingerprint data), which enables their unique identification or verification of identity;
- 1.4.7. **Profiling** – any form of automated processing of data that involves the use of data to evaluate certain personal characteristics relating to a natural person, in particular, to analyze or predict aspects concerning that person’s performance at work, economic situation, health, personal preferences, reliability, behavior, location, or movements.

2. Categories of Personal Data

2.1. Data Groups

The Bank processes, among others, the following categories of personal data:

2.1.1. Identification / Documentary Data

Name, surname, date and place of birth, sex, personal number, passport number, nationality, citizenship, signature, financial information, and other personal data. This data is used, in the first instance, for the initial identification of the client and for fulfilling “Know Your Customer” (KYC) and “Know Your Partner” obligations.

2.1.2. Contact Data

Actual and legal address, telephone number(s), email address, and other contact data. This data is used for communication and sending notifications.

2.1.3. Financial Data

Information on income (salary, rent, business income), monthly expenses, property (real and movable), liabilities, bank account balances, credit history, records of arrears, information on accounts held with other financial institutions, and other financial information.

2.1.4. Transactional Data

Bank account number, IBAN, history of transactions performed, card transactions, internet/mobile banking operations, transfers, payments, settlement orders, and other transaction-related information.

2.1.5. Contractual Data

Information on all agreements concluded with the Bank: credit agreement, deposit agreement, agreement on servicing with banking products, card usage terms, individual terms, amendments and addenda, and any other agreement.

2.1.6. Socio-Demographic Data

Education, profession and place of employment, political or public position, marital status, social status, and other socio-demographic data.

2.1.7. Digital / Technological Data

IP address, device ID, browser type and version, operating system, session logs (log files), cookies, internet/mobile banking usage behavior, geolocation, and other technological data

2.1.8. Biometric Data (Special Category)

Voice biometric sample (for telephone services), video-banking session recordings, facial recognition data (mobile banking authentication), behavioral biometrics. This data is processed only on the basis of the client's consent, in cases provided for by law.

2.1.9. AML/CFT / Financial Crime Data

Information on suspicious transactions identified through the monitoring of financial operations, results of automated transaction analysis, results of sanctions list screening, status verification, records of suspicious transactions, and other similar information.

2.1.10. Communication Data

Records of oral communication with the Bank (call center, video banking), email and SMS/MMS correspondence, chatbot session logs, complaints and records of their review, customer satisfaction survey results, and other similar data.

2.1.11. Open-Source / Public Data

Information from publicly available sources, including registries, court records, state sanctions lists, and other publicly available data.

2.2. Various Cases of Data Processing

2.2.1. Data of a Minor

The Bank processes the personal data of a minor, based on their consent, if they have reached the age of 16. Processing the data of a minor under the age of 16 is permissible with the consent of their parent or other legal representative, except in cases directly provided for by law.

Processing of a minor's special category data is permissible only on the basis of the written consent of their parent or other legal representative, except in cases directly provided for by law.

When processing a minor's data, the Bank always takes into account and safeguards the best interests of the minor. The consent of the minor, their parent, or other legal representative shall not be considered valid if the data processing endangers or harms the best interests of the minor.

2.2.2. Data of a Deceased Person

After the death of a data subject, the Bank processes their personal data only where there is an appropriate ground for processing established by law, and provided that the processing is not prohibited by the data subject's parent, child, grandchild, or spouse, except where the data subject prohibited, in writing, prior to their death, the processing of data concerning them after their death.

Processing of a deceased person's data is also permissible if 30 years have passed since their death, or where the processing is necessary for the exercise of a right related to inheritance.

Processing of a deceased person's name, surname, sex, and dates of birth and death is permissible regardless of the existence of the above-mentioned grounds and circumstances.

2.2.3. Biometric Data

Processing of biometric data by the Bank is permissible only where it is necessary for carrying out the Bank's activities, for security, for the protection of property, for preventing the disclosure of confidential information, or for ensuring information security and cybersecurity, and where achieving the relevant purpose by other means is impossible or would involve disproportionately significant effort.

Processing of biometric data is also permissible in other cases directly provided for by law and for the purposes and in the manner established by legislation.

2.2.4. Video Monitoring

The Bank's premises and service locations (including ATMs and cash desks) are subject to video monitoring, the purpose of which is to prevent and detect crime, protect security and property, protect confidential information, and/or perform tasks falling within the scope of other legitimate interests.

3. Purposes, Grounds, and Retention Periods of Processing

3.1. Legal Grounds

The Bank processes personal data where at least one of the following legal grounds exists:

- 3.1.1. Consent – the client has expressed consent to the processing of data.
- 3.1.2. Contractual obligation – processing is necessary for the performance of a contract concluded between the parties or for the conclusion of a contract;
- 3.1.3. Statutory obligation – processing is provided for by legislation (for example, AML/CFT, compliance with sanctions, reporting, etc.).
- 3.1.4. Public availability – the data is publicly available or the data subject has made it publicly available;

- 3.1.5. Vital interest – protection of the life, health, or other vital interest of the data subject or another person.
- 3.1.6. Public interest – processing is necessary for the protection of an important public interest;
- 3.1.7. Sphere of public interest – processing is necessary for performing tasks falling within the sphere of public interest defined by the legislation of Georgia, including for the purposes of crime prevention, crime investigation, criminal prosecution, the administration of justice, the enforcement of detention and imprisonment, the enforcement of non-custodial sentences and probation, operative-investigative activities, public safety, the protection of law and order, including ensuring information security and cybersecurity;
- 3.1.8. Legitimate interest – processing is necessary for the protection of a significant legitimate interest of the Bank or a third party, except where there is an overriding interest in protecting the rights of the data subject (including a minor);
- 3.1.9. Provision of service – processing is necessary to review an application submitted by the data subject and to provide the service to them.

3.2. Data Processing Table

The table below sets out the main categories of processing:

Category of Personal Data	Purpose of Processing, Including	Legal Basis	Retention Period
Identification / documentary data	Client identification, account opening, KYC/AML screening	One of the grounds provided for in items 3.1.1 – 3.1.3, 3.1.4-3.1.9	15 years from the end of the relationship
Contact data	Communication, sending notifications, contractual obligation	3.1.1-3.1.3, 3.1.8-3.1.9 One of the grounds provided for in the items	15 years from the end of the relationship
Financial data	Loan decision-making, creditworthiness assessment, portfolio management	3.1.1-3.1.3, 3.1.8-3.1.9 One of the grounds provided for in the items	15 years from the end of the contract
Transactional data	Performing banking operations, payment management, reporting	3.1.1-3.1.3, 3.1.8-3.1.9 One of the grounds provided for in the items	15 years from the end of the relationship
Contractual data	Preparation, conclusion, and performance of agreements	3.1.1-3.1.3, 3.1.8-3.1.9 One of the grounds provided for in the items	15 years from the end of the relationship

Socio-demographic data	Client segmentation, personalized offers, product creation/development	One of the grounds provided for in items 3.1.1-3.1.3, 3.1.5, 3.1.8, 3.1.9	5 years from the end of the relationship
Digital / technological data	Cybersecurity, fraud detection, UX improvement	3.1.1-3.1.3, 3.1.8-3.1.9 The ground provided for in the items	3 years from data collection
Biometric: voice recording, facial recognition (video banking, mobile banking)	Authentication, remote service	One of the grounds provided for in items 3.1.1, 3.1.5, 3.1.7, 3.1.8	2 years from termination of the relevant service
AML/CFT / financial crime data	Prevention of money laundering, terrorism financing, and sanctions non-compliance	The ground provided for in item 3.1.3	15 years from the end of the relationship
Communication: oral communication (recorded), email, correspondence	Business records, complaint handling, dispute resolution	One of the grounds provided for in items 3.1.2, 3.1.3, – 3.1.8, 3.1.9	15 years from the end of the relationship

3.3. Direct Marketing

The Bank processes a client's personal data for direct marketing purposes only on the basis of the client's prior, voluntary consent. Marketing communication may be carried out via SMS, email, push notifications, telephone calls, and/or other communication channels.

The data subject may withdraw their consent to the processing of personal data for marketing purposes at any time.

The data subject will, in any case, receive mandatory and/or contractual notifications (including notifications regarding changes in tariffs, new terms and conditions, and expiry reminders), which are not considered marketing communications.

3.4. Automated Decision-Making (Profiling)

The Bank may use automated decision-making, including profiling, for the following purposes:

- Deciding on loan applications, e.g., automated creditworthiness assessment;
- Fraud detection, e.g., automated transaction monitoring;
- Monitoring AML/CFT operations, e.g., algorithmic filtering of suspicious transactions;
- Client segmentation, e.g., generating personalized offers;
- Creation of personalized products tailored to a specific customer;

- Offering personalized products tailored to a specific customer.

The data subject has the right to: (a) request an explanation of the logic and results of an automated decision; (b) contest an automated decision; (c) request a review of the decision with human involvement.

The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them, except where a decision based on profiling:

- Is based on the explicit consent of the data subject;
- Is necessary for entering into a contract or for the performance of an already existing contract;
- Is provided for by law or by a subordinate normative act issued on the basis of law.

The use of special category data in automated decision-making is permissible only where one of the following grounds exists

- The data subject has given written consent to the processing of special category data for one or several specific purposes;
- Processing of special category data is necessary for the purposes of crime prevention (including relevant analytical research), crime investigation, criminal prosecution, the administration of justice, the enforcement of detention and imprisonment, the enforcement of non-custodial sentences and probation, ensuring the placement of a person in a temporary detention isolator, combating illegal migration, providing international protection, responding to administrative offenses, ensuring civil and fire safety, operative-investigative activities, public safety and/or the protection of law and order (including the conducting of criminological research by the relevant law-enforcement authority or court), and such processing of data is provided for by the relevant law or by law and a subordinate normative act issued on its basis;
- Processing of special category data is necessary for the protection of an important public interest,

and provided that adequate safeguards exist at the same time for the protection of the data subject's rights, freedoms, and legitimate interests.

4. Sharing Data with Third Parties

4.1. Grounds for Sharing

The Bank will share a data subject's personal data with third parties only:

- With the client's prior consent;
- For the purpose of creating, offering, and developing products;
- For the purpose of providing services;
- In cases provided for by legislation (court, investigative authority, banking regulator);
- For the performance of a contractual obligation (where providing the service requires sharing data);
- For the purpose of protecting the Bank's legitimate interest (dispute resolution, debt management, and other purposes).

4.2. Categories of Recipients

The Bank may share personal data with among others, the following recipients:

- The National Bank of Georgia – in the course of supervision, for reporting purposes;
- LEPL Financial Monitoring Service – in the course of supervision, for AML/CFT reporting purposes;
- The Ministry of Internal Affairs of Georgia / the Prosecutor’s Office – in cases defined by legislation;
- Tax authorities of Georgia – in cases defined by legislation, including when fulfilling CRS/FATCA obligations;
- Credit information bureau(s) – in cases defined by legislation;
- International and local payment systems (Visa, Mastercard, local systems) – for the purpose of processing transactions and providing card services;
- Correspondent/intermediary banks – for the purpose of carrying out international transfers;
- Insurance companies – for the purpose of servicing insurance products;
- IT/technology service providers (cloud, cybersecurity) – for the purpose of providing services and for the Bank’s operations;
- Legal, audit, and consulting organizations – for the purpose of receiving professional services;
- The Bank’s parent, subsidiary, and affiliated companies – for the purpose of providing services.

Data will be transferred to third parties under circumstances ensuring compliance with all requirements established by legislation, and such persons shall undertake an obligation to process the data in an appropriate manner.

4.3. International Transfer of Data

The Bank may transfer personal data outside Georgia, in particular:

- When carrying out international transfers via the SWIFT network.
- When using cloud providers located in the EEA/UK.
- When engaging with GDPR/UK GDPR subjects, in fulfilling FATCA/CRS obligations.
- For the purpose of providing services, and other purposes.

Transfer of personal data by the Bank to another state or international organization is permissible only in compliance with the requirements set out in the legislation of Georgia “On Personal Data Protection,” and where the relevant state or international organization ensures adequate safeguards for data protection and for the protection of the rights of the data subject.

Even in the absence of adequate safeguards, transfer of data is permissible in cases directly provided for by legislation, including where the transfer is provided for by an international treaty or agreement of Georgia, by the relevant legislation or a normative act, with the informed written consent of the data subject, or where it is necessary to protect their vital interests or to ensure an important public interest.

Transfer of data is also permissible where the Bank ensures adequate data protection safeguards through an agreement concluded with the recipient state, public institution, legal or natural person, or international organization. In such a case, the transfer of data shall be carried out only after obtaining the relevant permission of the State Audit Office, and the agreement must contain legally binding and enforceable terms.

When transferring data internationally, the Bank ensures that the organizational and technical measures necessary for the secure transfer of data are taken.

Further transfer to a third party of data already transferred to another state or international organization is permissible only where it serves the original purposes and satisfies the grounds for data transfer and the adequate data protection safeguards defined by legislation.

5. *Rights of the Data Subject*

5.1. *List of Rights*

In accordance with the legislation of Georgia, the client (data subject) has the following rights:

Right	Content	Response Time
Receipt of information	The right to know what data is being processed, for what purpose, on what grounds, the source of the data collection/acquisition, and the retention period or the criteria for determining it	10 business days
Receipt of information	The right to know the legal basis and purposes of data transfer, as well as information on adequate data protection safeguards, if the data is transferred to another state or international organization;	10 business days
Receipt of information	The right to know the identity of the data recipient or the categories of data recipients, including information on the grounds and purpose of the data transfer, if the data is transferred to a third party;	10 business days
Receipt of information	The right to know about a decision resulting from automated processing, including profiling, and the logic used to reach such a decision, as well as its impact on data processing and the expected/likely consequences of the processing.	10 business days
Access to data	Reviewing the data, obtaining a copy in electronic or written form free of charge	10 business days
Rectification, updating, and completion	The right to request the rectification, updating, or completion of incorrect, inaccurate, or incomplete personal data.	10 business days
Cessation of processing, erasure, destruction	The right to request the cessation of processing, erasure, or destruction of data	10 business days

Restriction of access to personal data	Where personal data is processed in a publicly accessible form, the restriction of access to such data and/or the deletion of copies of the data or internet links providing access to such data	10 business days
Right to data blocking	Where the accuracy or authenticity of the data is disputed, the data is no longer necessary for processing, the processing is unlawful, the matter is under review, or the data needs to be retained as evidence	3 business days
Right to data portability	Transfer of data in a machine-readable format (where technically feasible).	10 business days
Objection to processing (marketing)	The right to object to the processing of personal data for direct marketing purposes	7 business days (marketing)
Withdrawal of consent given	The right to request the termination of data processing based on consent at any time, without providing any explanation.	10 business days
Contesting an automated decision	Requesting a review of an automated decision with human involvement.	10 business days

The 10-day period established for receiving information, accessing or reviewing personal data, and/or obtaining a copy thereof may, in exceptional cases and with appropriate justification, be extended by no more than 10 working days. The data subject shall be notified of such extension without delay.

The data subject has the right to withdraw their consent at any time, without providing any explanation or justification. The Bank shall comply with the data subject's request in accordance with applicable legislation, provided that there is no other legal basis for processing the data besides consent. The withdrawal of consent shall not affect the Bank's right to process personal data on other legal grounds.

5.2. Exercising Rights

To exercise their rights, the data subject may:

- Visit any branch of the Bank;
- Send an application by email: privacy@ngbank.ge
- Use online banking or mobile banking;
- Contact the Bank's call center

The Bank ensures that the matter raised by the data subject is reviewed and resolved no later than within the timeframes established by legislation

The client may also file a complaint with the Personal Data Protection Service of Georgia – <https://pdp.sao.ge/ka>

6. Digital Channels and Cookies

6.1. Online Banking / Mobile Banking

When using the Bank's electronic platforms (internet/mobile banking), the following may be processed:

- Device ID, model, brand, name, OS version, and application version.
- Session duration, page navigation, operations log.
- IP address, geolocation
- Phone contact list;
- Other data for the purpose of providing services and ensuring security.

If the data subject uses a photograph in digital channels, the photograph will be visible to third parties when using the transfer functionality.

6.2. Cookies Policy

The Bank's website uses so-called "cookies" in the following categories:

- Essential Cookies — necessary for the functioning of the website; do not require consent.
- Functional Cookies — to improve the user experience;
- Analytics Cookies — for anonymous analysis of visitor behavior and to improve the website.
- Marketing Cookies — for personalized advertising.

The client may manage cookie settings via the cookie banner displayed on the Bank's website. The full cookie policy is available on the Bank's website.

7. Data Retention Periods

The Bank retains personal data for the period established, at a minimum, by legislation and/or for as long as a specific ground for retaining the data exists. The main information on data retention periods is set out in this Policy; if the Policy does not cover information on the retention period for any type of data, the data subject should contact the Bank's Personal Data Protection Officer.

8. Information Security

For the purpose of protecting customers' personal data, the Bank has implemented the best information security standards and systems. Taking a risk-based approach, the Bank uses, among others:

- Role-based access and the principle of least privilege;
- The principle of managing the authority of users and employees;
- Strong authentication;
- Protection of data during storage and transmission, including, where appropriate, encryption;

- Activity logging, security logs, and monitoring;
- Measures to protect network, system, and end-point devices;
- Secure configuration, updates, and vulnerability management;
- Backup copies, and recovery and continuity mechanisms;
- Rules for the secure storage and destruction of physical documents and media;
- Employee confidentiality obligations and regular awareness-raising;
- Periodic assessment, testing, and improvement of security measures.

9. Communication and Complaints

The Bank has a Personal Data Protection Officer (DPO)

For any matter related to data protection, the client may contact the Bank's DPO:

Name and surname: Mariam Maisuradze,

Email: privacy@ngbank.ge

Address: 138A Aghmashenebeli Avenue, Tbilisi, Georgia

Supervisory Authority

The client may also file a complaint with:

The State Audit Office of Georgia

Address: 0105 Tbilisi, 7 N. Vachnadze St.

Website: <https://pdp.sao.ge/ka>

Email: sao@sao.ge