BASISBANK

Data Protection Policy

Basisbank

TBILISI

2025

Contents

Chapter 1. General Information

1.1 Introduction

This Personal Data Processing Framework of JSC Basisbank (hereinafter referred to as the "Bank" or the "Framework") outlines the key principles governing the processing of personal data by the Bank and its branches. It has been developed in compliance with the Law of Georgia on Personal Data Protection and the General Data Protection Regulation (GDPR) of the European Union, ensuring the security and lawful processing of personal data.

This document updates and replaces all previous regulatory documents related to personal data processing within the Bank.

1.2 Purpose of the Document

Throughout the relationship between the data subject and the Bank, and even after its termination, the Bank processes various categories of personal data. The scope and purpose of this processing are strictly defined and adhere to the principles set forth in this Framework.

This document serves two key purposes:

It ensures that the Bank fulfills its legal obligations and responsibilities concerning data processing.

It enhances the service experience for customers, business partners, and other individuals defined in this Framework.

1.3 About Us

Joint Stock Company Basisbank (R/N 203841833) (hereinafter referred to as the "Bank" or "We") is a licensed commercial bank operating in accordance with Georgian law. As the entity responsible for processing personal data, the Bank is committed to ensuring compliance with data protection regulations.

1.4 Scope of the Document

This Framework applies to all individuals who interact with the Bank, including:

- Customers (potential, current, and former)
- Business partners
- Service providers
- Any other individuals connected to the Bank, its products, or its services (hereinafter referred to as you, the data subject) of JSC “Basisbank” who are in any way related to the Bank, the Bank’s products and services.

It covers all data processing activities where the Bank acts as a controller, processor, or co-processor. The Bank ensures that all personal data processing activities comply with this Framework.

Additionally, this document applies to all categories of data, systems, processes, and procedures involved in the Bank’s personal data processing activities.

1.5 Definitions

Biometric Data: Information related to the physical, physiological, or behavioral characteristics of an individual (e.g., facial images, voice patterns, or fingerprint data) processed through technical means for unique identification or verification.

Business Partner, Service Provider, or Supplier: Any third party that provides goods or services to the Bank in support of its operations, including vendors, consultants, contractors, and outsourcing partners.

Special Category Data: Special category data includes any personal information related to an individual's racial or ethnic origin, political opinions, religious, philosophical, or other beliefs, trade union membership, health status, and sex life. It also covers legal statuses such as being accused, convicted, acquitted, or recognized as a victim in criminal proceedings. Additionally, it includes information about convictions, sentencing, alternative legal measures, recognition as a victim of human trafficking or a crime under the Georgian law on the Prevention of Violence against Women and/or Domestic Violence, imprisonment, and execution of a sentence. Furthermore, it encompasses biometric and genetic data processed for the purpose of uniquely identifying an individual.

Customer: Any individual or entity that directly or indirectly establishes a business relationship with the Bank or uses its services, regardless of the nature, character and frequency of the service. This includes account holders, borrowers, co-borrowers, mortgage/pledge holders, depositors, investors, and any persons directly or indirectly connected to these relationships, such as family members, dependents, or emergency contacts.

Automatic Data Processing: The processing of data using information technology.

Data Processing: any operation performed on data, including collection, obtaining, access, photo taking, video monitoring and/or audio monitoring, organization, grouping, interconnection, storage, modification, recovery, retrieval, use, blocking, deletion or destruction, as well as disclosure of data through transmission, publication, dissemination, or making it available by other means.

Data Protection Regulation(s): all legislative and subordinate acts in force in Georgia in the field of data protection.

Semi-automatic Data Processing: processing of data using information technology and non-automatic means.

Data Subject: any natural person whose data is being processed.

Personal Data (hereinafter - "Data"): any information related to an identified or identifiable person. A natural person is identifiable when it is possible to identify them directly or indirectly, including through name, surname, identification number, geolocation data, electronic communication identification data, physical, physiological, mental, psychological, genetic, economic, cultural, or social characteristics.

[All terms in this document are used with the meaning provided by the Law of Georgia on Personal Data Protection.]

1.6. Basic Principles

In the process of personal data processing, the "Bank" is guided by the following principles:

- **Lawfulness, Fairness, and Transparency**: We process your personal data on legal grounds, fairly and transparently.
- **Purpose Limitation:** We process personal data for specified, explicit, and legitimate purposes. We ensure that your personal data is not processed in a manner incompatible with these purposes.
- **Data Minimization:** We strive to ensure the processing of minimal amounts of personal data, meaning we only process data necessary to achieve the specified purpose.
- **Accuracy:** We ensure that personal data is accurate and up to date. If data is inaccurate, we correct it immediately.
- **Storage Limitation:** Personal data must be kept only in a form that permits identification of data subjects for no longer than necessary for the purposes for which the data is processed. We ensure that data is safely and reasonably destroyed when storage is no longer needed.
- **Integrity and Confidentiality:** We strive to ensure data processing in a way that protects against unauthorized or unlawful access and processing, accidental loss, destruction, or damage.
- **Accountability:** We take responsibility to ensure that data processing complies with current data protection regulations and requirements set by the supervisory authority.

Chapter 2. Lawfulness of Data Processing and its Scope

2.1. Informing Data Subjects

The Bank ensures proper information to subjects about the main issues of personal data processing according to this document.

2.2. Categories of Personal Data

In its relationship with you, the Bank processes various categories of personal information, which is determined by the nature of the relationship, specific purpose and objective for which personal data is processed. Additionally, it is possible to process all or only some of the data specified in the relevant category (categories).

Identity	Such data includes, for example, your name, surname, age, gender, personal identification number, date of birth, place of birth, citizenship;
Contact	Contact information includes the following types of information - registration address, actual and/or legal address, email address, mobile and landline phone number, contact and dependent contact information for emergencies;
Financial	Such information includes information on your bank accounts (bank, internet bank, electronic wallet, account number, card number, etc.),

	information on tax status and credit status and history, transactions (transfers, deposits, withdrawals, purchases), data on your dependents and/or third parties, valuation of your property and other assets, information related to the insured product, your financial products and services, equity participation in enterprises, information about remote services;
Contract	Information about the products and services we provide to you within the framework of the relationship between you and us, information about the employment relationship (activity, employer, source of income and employment history), information about your relationships with third parties that you carry out through the Bank;
Information based on the requirements of the banking regulatory framework:	Information that the Bank needs for the purposes of conducting monitoring and compliance procedures, for anti-money laundering (AML) measures, information obtained within the framework of "Know Your Customer" (KYC).
Technical	Information about the devices and other technical details used by you within the framework of using our service, for example, Internet Protocol (IP) address, operating system, log records, information about your emails and accounts.
Location-related	Data related to your location, which the "Bank" may obtain through your mobile number or internet connection address.
Communication records	Communication established by you in your relationship with the "Bank", including emails, records of mail, letters, telephone calls.
Marketing preferences	Information about your choices regarding the means of receiving marketing communications, as well as information about the form of communication you prefer, information about your consent/refusal to the use of direct marketing mechanisms.
Risk management	Credit and non-credit risk assessments, information obtained from fraud detection activities and other information related to risk management, which may also fit into other categories.
Behavioral data	Information about details related to your behavior.

Audio/visual	Such information includes recordings of your telephone calls, recordings of video and audio monitoring systems, photographs, etc.
Usage-related	Information related to your use of our property.
Socio-demographic	Information about your citizenship, education, profession, workplace, family and any other related information, such as language, gender, age, marital status, etc.
Interactive	Information recorded by you during the period of communication with us, both physically and remotely, by telephone, by email, by filling out a physical form or through any other channel (including the use of social media).
Registers and other public information	Information about you that is registered and exists in various databases and/or is protected in public records (for example, at LEPL the National Agency of the Public Registry), as well as information about you that is openly and publicly available on social networks or otherwise;
Special category data	Information related to your racial or ethnic origin, political opinions, religious, philosophical or other beliefs, trade union membership, health status, status as accused, convicted, acquitted or victim in criminal proceedings, conviction, criminal record, diversion, imprisonment and execution of punishment against you, as well as biometric and genetic data that is processed for the purpose of your unique identification. We will only collect data in this category after you have expressed explicit consent to the collection of personal data, except in cases directly provided for by law where processing is possible without obtaining direct consent.

Please note that this list may be updated from time to time.

2.3 Collection of Personal Data

The Bank obtains personal data through various means. Basic information is collected based on the data subject's own provision of information. Your personal data will be provided to the Bank through application forms, mobile applications, and other devices such as ATMs. For example, when you contact us through any physical or remote channel, identification, contact, usage-related, and other data may be automatically shared from you. Considering the specifics of the request, including but not limited to account opening, loan taking, executing any other transaction (depositing, withdrawing, transferring,

opening deposits, or others), meetings, and consultations. When using internet banking, mobile applications, website analytics (e.g., "cookies"), additional financial, contractual, interactive, and other data will be collected.

Data may be collected based on information provided by "third parties," credit agencies, employers, service development agencies, financial institutions, risk management agencies, and software or other entities; in this case, the Bank ensures appropriate contractual protection guarantees when processing your personal data.

The Bank may obtain data from other publicly available sources, including public registry records, social networks, the internet, and website cookies.

Your data is also shared through email, physical mail, telephone recordings, and messages. Any form implemented by the "Bank" (application, consent, survey, feedback forms, etc.), your provision of identification or contractual documentation may be accompanied by sharing personal data with the "Bank." We assure you that we will process them in accordance with and based on this document, only for defined purposes and grounds.

Please note that if third-party data is provided (beneficiary, additional cardholder, guarantor, family member, employer, contact person, employee, staff member, or other), you are responsible for notifying and, if necessary, obtaining consent from the aforementioned persons before providing this information to us, for processing their personal data for the purposes defined in this document.

2.4. Cookies

Our website may use cookies, which are text files. They contain small amounts of information and are downloaded to your computer or mobile device when visiting a specific website. During each visit, cookies are sent back to the website from which they originated or move to another website that recognizes the cookie. Cookies are widely used to make websites function, or function more effectively, and provide information to website owners.

Cookies serve many functions, including helping with efficient navigation between pages, remembering preferences, and generally improving user experience. For example, cookies may indicate whether you've been to the website before or are a new visitor. They also ensure that advertisements/offers are delivered to you in a personalized manner.

Through cookies, we may collect information about your use of electronic services, such as application usage, file searches, user activity (e.g., pages viewed, time spent on specific pages, online page browsing, clicks, actions, etc.), timestamps, messages. Information will be collected for incident resolution purposes, as well as for research and analysis of your service usage.

You have the right to accept or reject cookies. Please note that by rejecting cookies, you may no longer be able to use our website's full functionality.

2.5 Basis and Purpose of Data Processing

2.5.1 Basis for Data Processing

Your personal data may be processed based on the following grounds:

- **Consent**: If the bank obtains your consent for processing personal data, this forms a legal basis for us to carry out the relevant actions until you withdraw this consent.
- **Contractual Obligations:** Your personal data may be processed to fulfill contractual or pre-contractual obligations necessary for conducting business and providing services. This includes any actions performed according to customer instructions, such as managing accounts, processing transactions, payments, deposits, loans, investments, and other banking services and transactions.
- **Legal or Regulatory Requirements:** Many of our data processing activities are based on legal and regulatory requirements. These requirements may stem from national or international regulations, including those related to commercial banks, the National Bank, financial institutions, anti-money laundering (AML), counter-terrorism financing (CTF), tax obligations, and client information collection duties.
- **Legitimate Interests:** We process your data to protect our significant legitimate interests. This includes managing and improving services, managing banking risks, marketing activities, exercising legal rights, managing disputes, ensuring the security of information systems, monitoring for fraud, and preventing and investigating crimes.

Data may also be processed based on other legal grounds as specified by law for appropriate purposes.

2.5.2 Purpose of Data Processing

The nature and scope of our relationship with you determine the purposes for which we process your personal data. The primary purposes include:

- **Customer Identification and Verification:** For this purpose, we may use identification, contact, transactional, socio-demographic, location-related, registry, public, biometric, "Know Your Customer" (KYC), audio-visual, interactive/documentary, contractual, and other relevant data.
- **Provision and Management of Banking Products and Services:** This may involve opening, maintaining, and closing bank accounts, processing banking operations, payments, deposits, withdrawals, transfers, utility payments, issuing and managing debit and credit cards, loans, currency conversions, and other transactions. In addition to identification data, processing financial information is crucial.
- **Risk Management:** As a financial institution, we are committed to maintaining financial stability, preventing and detecting criminal or fraudulent activities. Personal data processing is essential for risk assessments, including credit, operational, market, and liquidity risks.
- **Legal Compliance and Regulatory Adherence:** The Bank is a regulated business entity. The scope of regulation and compliance standards are established by both domestic and international legal acts. This may include compliance with Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) regulations, fulfillment of tax or other regulatory requirements, responding

to requests from law enforcement agencies, regulatory bodies and other government authorities, conducting sanctions screening and ensuring compliance.

- **Marketing Activities:** Processing personal data for this purpose is necessary for personalized offers and promotion of the bank's products and services. For this, in addition to identification data, we may need usage-related, marketing, and interactive data. For direct marketing purposes, we rely on your expressed consent, which may be obtained either independently or when agreeing to the banking service agreement and/or this document. Please note that consent to direct marketing is voluntary and is not a mandatory condition for receiving banking services.
- **Customer Service and Support:** We assist thousands of customers daily with accessing banking products and services, processing requests, and handling customer complaints.
- **Reporting, Analytics, and Business Development:** Processing your data helps us understand customer and bank needs and preferences, fulfill legal and contractual obligations, and develop our business strategies effectively.
- **Protection of Rights and Security:** We process personal data to protect our legitimate interests, including property rights and security, investigating crimes, ensuring network security, and effectively managing operational risks.

We are authorized to process your data for any other purpose specified by law but will not process it for purposes incompatible with the original data processing purposes.

Please note that certain aspects of our data processing procedures may involve automated, semi-automated, or non-automated methods. Some activities may be automated, while others may require manual intervention or human decision-making. We ensure that all processing activities, whether automated or not, comply with data protection regulations. If you have any questions, please contact us for further clarification.

2.6. Processing of Personal Data for Direct Marketing Purposes

The freedom to choose how your personal data is processed for direct marketing purposes is in your hands. Direct marketing refers to the direct and immediate delivery of information to the data subject via phone, mail, email, or other electronic means regarding the bank's goods, ideas, services, work and/or initiatives, as well as forming, maintaining, implementing, and/or supporting interest in image and social themes.

We believe that a customer who has a contractual relationship with the bank and receives banking services from it has a legitimate expectation to receive offers from the bank and learn about customized service conditions, while the bank has a legitimate interest in providing and improving banking services to existing customers. In case of losing this interest, the bank has several channels available to customers through which they can decline receiving marketing offers from the bank at any time. Instructions for declining are provided directly in communications and are also available through the bank's communication channels. The bank additionally regulates the terms of receiving marketing offers and the content of customer consent through the banking service agreement and/or this document, and if necessary, obtains independently expressed consent from the customer.

Please note that if you declined marketing communications, we may still contact you for non-marketing purposes. Additionally, we inform you that if you simultaneously represent a manager, representative, authorized person, and/or person associated in any other form with our existing and/or potential corporate customer, we are authorized to process your personal data as information related to the mentioned legal entity and use this information for providing services to the legal entity, including for direct marketing purposes.

2.6.1. Consent to Direct Marketing

Based on the consent document intended for direct marketing purposes, which may be independently obtained electronically, in the form of a material document and/or as a result of your agreement to the banking service agreement and/or the present document, we will be authorized to process your data for direct marketing purposes.

When you agree to the processing of your data for direct marketing purposes, this means you agree to the following text:

"I, the data subject, agree that JSC BasisBank may process my personal data for direct marketing purposes using any communication channel, such as contact, identification, transactional, financial, socio-demographic, interactive, and geo-location data. I understand that this includes the following and is carried out as follows:

- Information about current/planned promotions and offers at the bank, which may include information about both banking products directly and services/offers/promotions of the bank's partner companies related to these products;
- The bank's marketing offer may be made through any communication channel(s) available to the bank, including (but not limited to) notifications in banking service channel(s) (internet banking, mobile banking), sending SMS to the client's contact phone number or making phone calls, and/or sending notifications to email addresses;
- My expressed consent is indefinite, however, I have the right to withdraw consent at any time and request the bank to stop processing my data for direct marketing (advertising) purposes by registering the corresponding request via email: info@basisbank.ge, call center *9292, or at a branch;
- The bank is obligated to stop processing the relevant data for direct marketing purposes no later than 7 (seven) working days after my proper request, after which I will not receive bank offers regarding banking services and products;
- Consent to data processing for direct marketing purposes is voluntary, and providing consent is not a mandatory prerequisite for the bank to provide me services;
- By giving consent, the bank will be able to offer products, services, various promotions, however, consent does not obligate me to use the bank's services;
- In case of withdrawal of consent and/or refusal, I understand that the bank will be unable to inform me about current promotions, products, and other services."

2.6.2. Right to Refuse Direct Marketing

We respect your choice. If you do not wish to receive direct marketing communications from us, you have the right at any time, without any fee or other restriction, to exercise the rights provided by law for data subjects, including the right of withdrawal (refusal of consent). **To do this, you should contact us via email at info@basisbank.ge at any time, through the call center at *9292, or through a branch. In case of refusal, we will immediately, but no later than the period established by law, stop sending you marketing communications.**

2.7. Processing of Special Category Data

- The personal data we hold about you may include your special category data related to:
- Your racial or ethnic origin;
- Political opinions, religious, philosophical, or other beliefs;
- Trade union membership;
- Health condition;
- Status as accused, convicted, acquitted, or victim in criminal proceedings, conviction, criminal record, diversion, recognition as a victim of human trafficking or crime under the "Law of Georgia on Prevention of Violence against Women and/or Domestic Violence, Protection and Assistance of Victims of Violence," imprisonment and execution of punishment;
- Biometric and genetic data.

We process special category data only for specific purposes and on grounds derived from data protection regulations, considering our or third parties' legitimate interests. Data processing is mainly related to fulfilling legal requirements, ensuring security, and providing customized services to customers, including but not limited to:

- **AML Compliance:** Banks are required to verify their clients' identity and monitor transactions to detect and prevent money laundering and terrorism financing.
- **Risk Assessment (including credit) and Monitoring:** The bank assesses customers' creditworthiness when offering loans or credit facilities. This may include analyzing sensitive information such as income, employment history, and health records to determine lending-related risks.
- **Fraud Prevention and Security:** The bank collects and analyzes special category data to detect and prevent fraudulent activities, such as unauthorized access to accounts or identity theft. This may include processing biometric data for authentication purposes.
- **Provision of Specialized Services:** Some banking services, such as insurance or property management, may require processing special category data to assess risk, determine eligibility, and customize services to individual needs.

- **Legal Obligations:** The bank may be legally required to collect and process special category data for various purposes, such as tax reporting, regulatory compliance, or responding to law enforcement requests.

2.8. Processing of Biometric Data

To receive and use our services through remote channels (internet/mobile banking, website www.bbcredit.ge), our regulatory framework requires us to perform electronic identification and verification of clients. Within this process, using software products (technical support), we collect your personal data, including biometric data, i.e., physical data (for example, facial image) that allows for unique identification or verification of identity of the subject.

For the electronic identification and verification process, we use Identomat Inc[1] (ID (SR 20204194256; n7977895), address: USA, 60 Hazelwood Dr, Champaign, IL 61820) software product that allows us to compare photos and verify document data through the process of taking photos of identification documents and dynamic selfies. This way, the bank verifies the client's identity and authenticity. Biometric data is processed for the following purposes:

- Security, prevention of fraud, disclosure of confidential information, and other illegal activities;
- Fulfillment of obligations imposed by law on the bank as a regulated entity;
- Receiving a simple and improved service experience.

Data processing takes place in Georgia and in jurisdictions that fall under the General European Regulation on Personal Data Protection (GDPR). Additionally, we conduct constant monitoring of biometric data processing activities and take appropriate organizational and technical measures to ensure data security.

By reviewing this document, you acknowledge and agree that the data processed by the bank may contain special category data, including biometric data, on the grounds specified above. We ensure their security.

Your personal data will not be accessible to third parties (except those who provide us with relevant services and for whom such information transfer is necessary) without your explicit consent as a data subject, unless required by law.

You acknowledge that you have the right to withdraw your consent at any time in accordance with the rules established by this document. However, withdrawal of consent will not affect any processing of special category data that occurred before the withdrawal of consent.

[1] Data processing and storage takes place on a secure server in Frankfurt, Germany. Remote server service providers are DigitalOcean LLC (https://www.digitalocean.com/legal/terms-of-service-agreement/) and Amazon Web Services (data protection terms are located at https://aws.amazon.com/legal/?nc1=f_cc).). The data is located in the European Union territory and complies with GDPR requirements.

2.9. Processing of Minors' Data

We process data about minors based on their consent if they have reached the age of 16, while processing data about minors under 16 requires consent from their parent or other legal representative, except in cases directly provided by law, including when data processing requires consent from both the minor aged 16 to 18 and their parent or other legal representative. As for special category data about minors, we process it only based on written consent from their parent or other legal representative, except in cases directly provided by law.

We take reasonable and adequate measures to verify the existence of consent from a parent or other legal representative of a minor under 16.

2.10. Data Protection Priority - Privacy by Default & Privacy by Design

“Privacy by Design” means implementing appropriate technical and organizational measures to protect the rights and freedoms of data subjects when determining the implementation of latest technologies, nature, scale, context, and purposes of data processing. Privacy by Default means implementing technical and organizational measures that ensure processing only the data necessary for a specific purpose.

The bank ensures protection of personal data in all its systems, processes, and services. Collected data is processed only for specific purposes and when there is a legal basis. Access to personal data is restricted as needed to authorized personnel, and unauthorized access control is continuously maintained.

We ensure appropriate technical and organizational measures are taken to protect your personal data from the initial stage of creating a new product or service.

2.11. Data Subject Consent

Data processing activities, in some cases, require data subject consent. The bank ensures obtaining such consent during data collection and, when possible, before processing. If a new processing purpose arises, the bank ensures updating consent from the data subject.

You, as a data subject, by reviewing this document, consent that within the scope of your relationship with the bank and arising from it, by applying for our banking or non-banking services or using them either once or multiple times, you agree to the processing of your personal data by JSC "BasisBank" for the purposes listed in the "Purpose and Basis of Data Processing" chapter of this document. You have reviewed our framework regarding data processing, which provides you additional details about how we process your personal data, and you have the right to withdraw your consent at any time without any fee. Please note that refusing personal data processing may affect our ability to provide certain services or prevent their use. Using our services implies your ongoing consent to personal data processing in accordance with this document until it is withdrawn.

2.12. Automated Individual Decision-Making

Certain processes in the bank, such as credit scoring, fraud detection, risk assessment, and lending decisions, may be automated. This includes profiling. In automated processes, the bank regularly monitors the algorithms used, ensures human involvement upon request (except in cases of legal exemption), and creates appropriate guarantees by giving data subjects the opportunity to express their opinion and appeal decisions.

Automated decisions are made in accordance with current data protection legislation and are based on principles of fairness, transparency, and accountability.

Persons subject to automated decisions have the right not to be subject to decisions made solely by automation, including profiling, which creates legal or other significant consequences for them, except when decision-making based on profiling:

a) Is based on the data subject's explicit consent;

b) Is necessary for entering into or performing a contract between the data subject and the person responsible for processing;

c) Is provided for by law or by a subordinate normative act issued within the scope of authority delegated by law.

By reviewing this framework, you as a data subject acknowledge that JSC Basis Bank in certain cases, such as credit scoring, fraud detection, lending decisions, and risk assessment, uses automated decision-making processes, including profiling. You acknowledge that automated decisions may significantly affect you, for which you have additional rights defined by law and this document regarding such decisions. You have the right to refuse data processing for this purpose at any time without any fee. Please note that refusing personal data processing in the automated decision part may affect our ability to provide certain services or prevent their use. Using our services implies your ongoing consent to such processing of personal data in accordance with the framework until it is withdrawn.

2.13. Data Storage

The bank stores your personal data only for the period that does not exceed the time necessary for the purposes of processing. At the same time, since the bank is a regulated entity, certain data storage may also be determined by legal terms. Our general principle is that the bank keeps personal data related to customers and business partners throughout the duration of the contractual relationship and the legal limitation period, during which the bank or data subject requests this information for legal actions or for the period necessary to properly fulfill obligations imposed by law.

We store your personal data on secure data servers located both at the bank's physical locations in Georgia and in cloud environments (for example: AWS Amazon Web Services, Microsoft Azure) whose servers are located in countries with adequate personal data protection guarantees and whose security is ensured in accordance with GDPR requirements. Access to information stored on the server is strictly limited and

only possible as needed. Some information is stored on email addresses and their movement is strictly controlled. Internal regulations establish the responsibility of persons with access.

Although we take all reasonable measures to protect your personal data, we advise you to exercise caution when sharing personal data in electronic format, additionally notify us of instances of providing special information, and ensure additional security when using digital channels from your own devices.

2.14. Data Subject Rights

- As a data subject, you have the following rights:

- Right of access: Data subjects have the right to request access to their personal data and information about how it is processed; they are authorized to request information from the company about the processing of their data.

- Right to rectification (update and completion): Data subjects have the right to request correction, updating, and completion of inaccurate or incomplete personal data.

- Right to withdrawal: Data subjects are authorized at any time, without explanation, to withdraw (request cessation of data processing and/or destruction of processed data) their consent given to the "Bank" regarding the processing of their personal data. Please note that withdrawal of consent does not invalidate the legal consequences arising within the scope of consent before its withdrawal. Additionally, in case of consent withdrawal, we may be unable to provide you with complete service.

- Right to restrict processing: Data subjects have the right to request restriction of their personal data processing.

- Right to data portability: Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format and transfer it to another processor.

- Right to complain: If you believe your personal data is being processed in violation of legal requirements, you have the right to contact the Personal Data Protection Service of Georgia. For more information, you can visit the Service's website at https://personaldata.ge/.

- Other rights provided by law: Your rights are detailed in the Law of Georgia on "Personal Data Protection," therefore, it is recommended that you familiarize yourself with it additionally.

2.15. Ways to Exercise Rights

Since proper management of personal data and protection of data subjects in this regard is important to us, we have appointed a Personal Data Protection Officer. If you wish to exercise any of your rights granted by this document and current regulations, or have any questions/comments about how we process your personal data, please contact us at the following contact details:

- Email: dpo@basisbank.ge
- Phone: 032 2 922 922
- Address: 1 Queen Ketevan Ave., 0103, Tbilisi, Georgia

Upon receiving your message, our officer will confirm receipt within 3 (three) working days and provide you with an estimated timeframe needed for investigating and reviewing your request. If specific timeframes are established by current legislation for exercising your rights, we will ensure compliance with them. Additionally, you will not be required to pay any fee for notifications, access to your personal data, or exercise of other legal rights, except for cases established by legislation (for example, if fees are provided by law and/or established due to resources spent on providing data in a form different from the storage form or due to frequency of requests). In case of unreasonably frequent submission of requests by the data subject, we reserve the right to refuse their execution.

Our goal is to provide comprehensive answers, including details of any actions taken, conclusions, or results. If you are not satisfied with our response or think that your rights regarding data processing have been violated, you have the right to contact the supervisory authority, the Personal Data Protection Service (for additional information, you can visit the Service's website at https://personaldata.ge/). However, as a sign of our loyalty to you, we ask that you first communicate with us regarding any issues.

Please note that we may need specific personal information from you to help identify you and process your request. This is a security measure to prevent disclosure of personal data to unauthorized persons. We may also contact you for additional information regarding your request to expedite the provision of response information.

Chapter 3. Management of Data Processing Processes

3.1. Data Security

The Bank takes appropriate organizational and technical measures to prevent possible and associated risks of data processing. Such measures include, among others, logging data access (log records), information security mechanisms (confidentiality, integrity, availability), data pseudonymization, and others. It addresses the prevention of data loss, illegal processing, including destruction, deletion, modification, disclosure, or use threats.

The Bank's information technology structure is constantly being refined to create maximum security guarantees for your personal data.

We ensure maximum protection of the information you provide; however, you are responsible for the accuracy and reliability of the information you provide. In case of changes to this data, you can notify us about the change, and we promise to respond accordingly and reflect the change in the databases within a short period of time.

3.2. Data Security Breach

A data security breach (incident) is an event that causes unlawful or accidental damage, loss, as well as unauthorized disclosure, destruction, modification, access, collection/acquisition, or other unauthorized processing of data.

The Bank effectively responds to incidents considering appropriate technical-organizational measures and evaluates them according to the following criteria:

- Type/category of violation
- Nature, sensitivity, and volume of personal data
- Possibilities of data subject identification
- Severity of consequences
- Specific characteristics of the data subject
- Number of interested data subjects

All incidents of personal data breaches are recorded in a corresponding document that includes all details of the incident, including date, actions taken, participating parties, and action plan. Incident notification is made to data subjects and the supervisory authority no later than 72 hours when the personal data breach may pose a risk to the rights and freedoms of subjects.

3.3. Third Party Access to Personal Data

The Bank enters into contractual relationships with third parties within its activities. In this case, the Bank is the person responsible for data processing, while third parties may be involved in the processing process as authorized processors or co-processors. The Bank shares responsibility with them for each case of personal data processing, which is why we ensure the creation of appropriate security guarantees for all such processing, including through written contracts.

Moreover, we try to maximize the restriction of personal data distribution to third parties at an individual level, however, certain products and services cannot be received by the Bank without third party involvement. Accordingly, it needs to enter into contractual relationships with third parties operating both within Georgia and outside its borders. For example, these include IT direction (software product and provision (software and application) providers), legal, logistics, postal service providers) and other persons (business partners). Accordingly, they may have access to your personal data with specific purpose and limited functionality.

For example, the Bank may receive or transfer information about you, both actively and passively, to the following third parties:

- International payment system operators (such as VISA Inc. and MASTERCARD Inc. and/or their contractors) who help us manage your accounts and provide services;
- Payment service provider(s), identification-performing organizations, correspondent banks, or other third parties related to local and international transfer systems, payment service provision, and person identification/verification processes;
- For electronic signing of banking documentation within banking services, Signify LLC (ID 405432580; Address: 40 J. Shartava Street, Tbilisi, Georgia) through their platform "Signify";
- Organizations conducting anti-terrorism financing and anti-money laundering activities in Georgia and abroad;
- International and local money transfer service providers;
- Bank's business partners who perform outsourced operations for us, including auditors, financial and legal advisors, IT service providers, analysts, marketers, real estate appraisers, auditing, research, enforcement, consulting, and research organizations;
- Credit information bureaus to enable us to review applications and provide services based on analysis of your solvency and risk assessment. For example, in cases provided by law, the Bank is authorized to transfer your credit/non-credit and other relevant information to JSC "Credit Information Bureau Creditinfo Georgia" (ID 204470740), which will be available to credit information bureau users according to established law (lending organizations and information receivers/providers). Information to be transferred to the bureau is defined by law and, without limitation, may include: your identification, financial, contractual data, information about your current, fulfilled/unfulfilled obligations' volume and terms, information about security measures, guarantee-related information, and others;
- Public and private institutions: supervisory bodies, courts and other dispute resolution institutions, investigative and enforcement bodies, state or local self-government bodies. These include (non-exhaustively) the National Bank of Georgia, Personal Data Protection Service, Social Service Agency, National Agency of Public Registry, Public Service Development Agency, Deposit Insurance Agency, Revenue Service, Ministry of Internal Affairs of Georgia, and others;
- Bank's payment system user contractors (billing services), problem asset management companies, or collection organizations;
- Insurance companies;
- Postal and courier companies;
- Bank's partner entrepreneurs and other contractor companies - commercial entities using the Bank's POS-terminal services under contract with the Bank, partner development companies, organizations using salary programs;
- Communication network operators, SMS service provider companies that help us with direct marketing processing;
- Financial institutions (both in Georgia and abroad);
- Any other person for whom data sharing or information requesting serves a specific purpose, is established by regulatory requirements, or is necessary for ensuring compliance with contractual requirements with the relevant organization, as well as for fulfilling the Bank's duties related to audit/monitoring implementation, or serves to protect the Bank's legitimate interests.

The confidentiality of personal data is ensured by the receiving third party, and the Bank is not responsible for the breach of confidentiality by the information receiver unless otherwise provided by law.

Additionally, your personal data may be shared with organizations or services ensuring information security and cybersecurity or defense, public security. We allow access to your personal data in a maximally targeted and limited manner.

Categories of data that may be shared include, but are not limited to, contact and identification, contractual and interactive, technical, and marketing data. We take all reasonable measures to create appropriate guarantees to protect your personal data before receiving or sharing your data.

This list is not exhaustive and may be updated from time to time. In case of any questions regarding these matters, we will ensure your individual consultation.

3.1.1. International Transfer

Our main activities are conducted with the help of our internal or Georgia-based companies. However, there are cases of international transfers, during which we take appropriate technical-organizational measures to ensure the protection of your personal data:

- Data transfer agreements: We ensure the conclusion of appropriate agreements to ensure that foreign service providers process your personal data in accordance with data protection regulations in force in Georgia and this framework.

- Standard contractual terms: Where necessary and where individual contracts cannot be formed, we bind third parties with standard contractual terms related to personal data protection to ensure an adequate level of protection for your data.

- Data minimization: We transfer the minimum amount of personal data necessary for a specific purpose, and we ensure that access to your data is limited to authorized persons as required by legitimate interests.

- Security measures: We use various technical and organizational security measures to protect your personal data during transfer and storage, regardless of their location.

Our relationship with third parties is governed by agreements that include appropriate guarantees for personal data protection.

3.2. Video and Audio Monitoring

To protect our legitimate interests, prevent crime, detect/investigate it, protect public safety, personal security and property, protect confidential information, and perform other important tasks, video monitoring of external and internal perimeters of building(s), including service areas and workplace(s), is conducted at the "Bank's" physical locations in compliance with the requirements established by the Georgian Law on "Personal Data Protection."

During telephone communication with the Bank's representative, incoming and outgoing calls are recorded/processed through the call recording system (audio monitoring) for the purposes of service improvement and proper performance, review and response to applications and complaints, as well as protection of our other legitimate interests (including creating legally valid evidence) in compliance with the requirements established by the Georgian Law on "Personal Data Protection."

Video monitoring is carried out 24/7. In normal cases, video monitoring materials are stored for 30 (thirty) days from the moment of recording, or for the period necessary to achieve a specific purpose, while audio monitoring materials are stored only for the period necessary to achieve a specific purpose, after which they are subject to destruction unless there is a need and legal basis for longer-term data storage.

For your information, appropriate warning signs are placed in visible locations, containing information about both video and audio monitoring. All appropriate effective and adequate organizational-technical measures have been taken to prevent illegal/accidental disclosure of data reflected in recordings (both video and audio), their undesirable use, distribution, and others, including:

- Physical security of the monitoring system is ensured; the monitoring system and relevant technical equipment are located in secure rooms where only persons with appropriate authorization are admitted;

- Access to recordings is granted only to a defined circle of employees, whose access level and scope are determined considering employee functions and their professional need for access to recordings;

- Appropriate measures are taken for system information security to prevent unauthorized access from the internet and computer network;

- All actions performed on data in monitoring systems are fully recorded;

- All cases of disclosure of recordings are recorded.

As a rule, we do not allow third-party access to video and audio monitoring recordings. If cooperation with law enforcement agencies is necessary for a specific purpose, we may share such data with them when legal grounds exist. For example, if an incident occurs involving damage or destruction of our property or building, or violence or abuse towards customers, personnel, or security staff, we may share video and audio monitoring materials with law enforcement agencies on our own initiative to protect our legitimate interests. We may also share frames or photo materials with our internal or external advisors (including lawyers, consultants, insurance companies) as may be necessary to protect our legitimate rights and interests.

By being present at our physical locations, you agree to the collection and processing of your personal data through video and audio monitoring systems for the above-listed purposes. We take appropriate measures to protect the confidentiality and personal data of persons recorded in video and audio recordings, and access to such data is restricted to authorized personnel only. Recorded data is stored for a limited duration as necessary to achieve the purposes for which it was collected. They are stored securely and destroyed in accordance with current data protection regulations.

Chapter 4. Final Provisions

4.1 Changes and Updates

The "Bank" reserves the right to change or update this document at any time. We recommend periodically reviewing the framework for data processing to stay informed about how we process and protect your personal data. Any updates or changes to this document will be posted on our website. Continued use of our services implies that you are subject to the updated/revised framework for personal data processing and confirms your acceptance of it.

The provisions of this document also apply to individuals associated with the bank who are responsible for data processing, authorized for data processing, and responsible for data co-processing.

Your confidentiality and the responsible processing of your personal data are important to us. Therefore, we are ready to assist with every step taken to ensure data security.

1 St. Queen Ketevan Ave., Tbilisi, Georgia
+995 322 922 922
info@basisbank.ge