Personal and Bank Data Privacy Policy

Who we are

JSC ProCredit Bank is a joint-stock company established and operating in compliance with the laws of Georgia (TIN 204851197) and holding Banking Licence #233 issued by the National Bank of Georgia on 13 May 1999, with its registered address at 21, Al. Kazbegi Avenue, Tbilisi 0160, Georgia (hereinafter referred to as the 'Bank', 'we', 'our').

Document purpose

We believe that your trust depends to a significant extent on our ensuring the security of your personal data. Therefore, to maintain your trust, protect your rights and fully comply with the principles of the law, the Bank is committed to developing and implementing appropriate technical and organisational security measures. The Bank's personal data privacy policy, which complies with both local and international requirements, ensures that your personal data is processed legally, fairly, and transparently, without violating your dignity, for a clearly defined, legitimate purpose and in compliance with high-security standards. To protect data security, the Bank has adopted the technical and organisational measures during data processing that adequately ensure data protection, including against unauthorised disclosure, modification, access to them and their improper collection/retrieval, accidental loss, destruction and/or damage, or unauthorised or illegal processing.

In today's digital epoch, with the Internet being accessible everywhere and for all, the Bank is not just a physical place but a space that operates more effectively in an online environment with the help of up-to-date technologies. With regard to the importance of technological advances, JSC ProCredit Bank has developed new opportunities for customers, offering them fast and simplified ways of using flexible and safe bank services through myDirect and other remote channels that bring your bank together into a single digital zone. Along with new opportunities, the Bank is firmly committed to protecting the security of bank services and customers' personal data.

The Bank offers customers services through various digital/electronic channels. For instance, the Bank can offer services under a platform called myDirect, but each service is subject to the same data privacy terms and conditions as defined in this document.

This document outlines the principles, goals, and legal foundations that guide our processing of your personal data. It also defines how the law safeguards data subject rights

and regulates data processing under Georgian legislation and the EU General Data Protection Regulation.

This policy (hereinafter—the Policy) fully applies to the Bank and is based on internationally recognised fundamental data protection principles. It ensures that all the framework conditions are in place for internal or cross-border data exchange by the Bank, its subsidiaries, affiliates, and other partners.

The Policy ensures an adequate level of protection defined by Georgian legislation during the internal and cross-border exchange of personal data, including in countries that do not have national data protection legislation.

What is data, what kind of data do we process about you, and why do we process data?

In this document, 'data' refers to an individual's bank, commercial, and personal information.

'Personal data' means any information about a specific individual who can be identified either directly or indirectly. This could include an individual's identification by their name, surname, identification number, geolocation data, electronic communication data, physical, physiological, mental, psychological, genetic, economic, cultural, or social characteristics.

'Bank information' means any information on any payment transaction (including attempted transaction) performed, any account, any transaction performed from the account, and the account balance.

'Commercial information' means any information relating to the economic activity of a person which is of commercial value and whose disclosure may harm the person's commercial interests.

'**Data processing'** means any operation performed on personal data, including collecting, obtaining, accessing, photographing, video monitoring and/or audio monitoring, organising, grouping, interconnecting, storing, altering, retrieving, requesting for access, using, blocking, erasing, or destroying, and disclosing by transmission, publication, dissemination or otherwise making available.

The Bank ensures that your data are processed fairly and legally, only to the extent necessary to accomplish the relevant legal, legitimate, and/or specific goal.

JSC ProCredit Bank processes data in compliance with the Law of Georgia on Personal Data Protection, the relevant regulations of the National Bank of Georgia and the accepted international best practices.

The Bank processes various types of personal information, which may include, but may not be limited to, data from the following categories:

Identification data:

Name, surname, date of birth, personal number, identity and/or citizenship document data, gender, citizenship, place of birth, nationality, photograph, specimen signature.

Video images and photographs used to provide services through an automatic identification process.

Contact data:

Address (legal and actual), email, mobile and landline phone numbers, and contact person(s) information.

Document data:

Identity card, passport, driver's license, birth certificate, certificate of compatriot living abroad, residence certificate, temporary identification certificate, extract from the National Agency of Public Registry, document confirming the right to representation, etc.

Socio-demographic data:

Information about job/profession, citizenship, education, social status/income, etc.

Financial data:

Information about the economic and financial status; information related to transactions (including place and date of transactions) and accounts; credit history and solvency; information about arrears, financial products, income, property and other assets, payments and/or transfers.

Contract data:

Information about the products and services provided by the Bank.

Transaction data:

Payment (bank, e-wallet) information, account number, payment statement, balance, deposits, withdrawals, transfers, and other information related to accounts and transactions.

Interactive data:

Information obtained through face-to-face communication at the Bank, filling out hardcopy forms, by phone, e-mail and other channels (including social media).

Marital status, family member data

Marriage certificate, identification and document data of family members, information about family members/contact persons, information about a person's death, death certificate, inheritance certificate, etc.

Data on technological devices

IP address, cookies, application logs, behavioural data, location information, and details about how you use our products and services.

Technical data

Information about the device and technology you use for our services (computer or phone IP address, operating system, log records).

Location data

Data about where you are. For example, information collected through the location-specific features of your mobile device when you request services that depend on your physical location.

Audio and visual records

Video and audio monitoring system records and photographs.

Public data

Information obtained from public sources (for example, from the LEPL National Agency of Public Registry) and information that the data subject has otherwise made openly available.

Special category data

data connected to a person's state of health, criminal history, administrative detention, recognition as an accused, and biometric data such as facial images, etc.

Data, which the Bank has the statutory obligation to process

The data we are obliged by law to process (for example, data processed for the purpose of identification/verification, KYC, AML), etc.

Data about minors

The Bank processes data about minors based on the consent of the minor if he has reached the age of 16 and with the consent of his parent or other legal representative, except for cases directly provided by law.

Data about the deceased

The Bank processes data about the deceased only if there is a basis provided by law.

Biometric data processing

To access banking services remotely, you will need to complete an electronic identification and verification process in compliance with the laws. During this process, JSC Procredit Bank Georgia will collect and process your personal data, including special category (biometric) data, with the help of technical support. Online identification aims to ensure

that customers can be unmistakably identified to access the required banking services, simplify the customer service process, and facilitate electronic identification/verification. The Bank utilises specialised software for online customer service, and biometric identification is carried out through the Identomat system, which involves a visual record and a photograph.

During the electronic identification/verification process, the Bank uses technical support (the **Identomat**) to verify the person's authenticity. This verification involves taking a video and a dynamic selfie using the Identomat to ensure that there is a live individual on the other end of the camera and that no mask, photo, mannequin, or other means are being used. Your data is then compared with the photo on the presented identification document.

It should be noted that Identomat uses web services whose servers are located in the territory of the European Union and in the states whose activities comply with the requirements of the GDPR. The data placed on the above server resources is encrypted, and the providers of the server resources do not have access to the data content.

Cookies

We are constantly working to enhance the quality of service and experience on our website in order to ensure your safety. To achieve this, we collect the so-called cookies when you use our website and other remote platforms. Cookies are small text documents or pieces of code that typically contain a unique identification code. When you visit a website or use a mobile application, your computer requests permission to store this file on your device and access the information. The information gathered through cookies and similar technologies may include the date, time, and usage of a specific website or mobile application.

Our website uses cookies to keep you logged in and ensure smooth operation. Cookies also help us understand how our website is used and how we can make improvements. Additionally, cookies are used to display personalised ads based on your interests.

The Bank uses various types of cookies, including essential cookies, performance cookies, functional cookies, advertising/tracking cookies, and unclassified cookies.

Please take a moment to review our cookie policy. You have the choice to accept or decline the use of cookies and select specific types of cookies based on your preferences. If you wish to block cookies, you can adjust your browser settings. Keep in mind that blocking cookies may impact your ability to access certain technical features of the website, potentially affecting your overall user experience. For additional guidance on adjusting cookie settings, consult your browser's "Help" section.

Purpose of data processing:

The Bank processes your data only for legal and legitimate purposes and only in proportion to the relevant purpose based on the content of the relationship. Your personal data is processed only for the following purposes:

- Providing, improving, and developing any type of bank services for you (including providing remote services).
- Fulfilling the obligations arising from contractual or pre-contractual relations with the Bank.
- Providing you with information on any type of bank services.
- For direct marketing purposes, with your consent, offering you any kind of banking services/products, developing and planning marketing activities.
- Analysing your solvency.
- Monitoring the current credit product.
- Providing credit services to or monitoring the current credit product of a person financially related to you.
- Updating, correcting, or filling data.
- Sending or delivering the appropriate message/correspondence to the customer.
- Making sure bank processes/activities are in line with the laws.
- Preparing different statements, consulting on/conducting studies/services, and drafting reports for the Bank's purposes.
- Giving regulators or other supervisory bodies and audit companies access to data in accordance with the law.
- Reporting to the Bank founders.
- Taking part in various promotional games (relating to VISA, MasterCard, and other bank services).
- Allowing the Bank to discharge its statutory duties.
- Combating money laundering and terrorism financing, preventing financial crimes, and identifying, investigating, preventing and avoiding fraud and any other acts punishable by law.
- Ensuring the protection of our and your property and safety.
- Safeguarding the legitimate interests and/or legal rights of the Bank.
- Other cases stipulated by law.

Grounds for data processing:

Your personal data are processed only on the following ground(s):

- Your consent.
- Data processing is provided for by law.

- Data processing is required for the Bank to discharge its statutory duties.
- To safeguard the Bank's lawful/legitimate interests.
- Your application for services.
- To fulfil contractual obligations or enter into a transaction with you.
- Public availability of data.

Please note that the customer must provide relevant data to receive bank services. Otherwise, the Bank may refuse or even stop providing services.

How do we collect your data (sources)?

The Bank collects data directly from you and from third parties if they are in a contractual relationship with the Bank, and the release of information is provided for by law.

The Bank collects data directly from you:

- During your visit to any branch as well as through the Bank website or remote channels. Namely, we process personal data when a person seeks services from us and/or becomes our customer, fills out an online application form, signs up for a service or signs up for our online services, signs a contract, uses our products or services, or contacts us through any of the Bank's remote channels including sending us letters by mail or e-mail.

The Bank collects data from the following third parties/organisations/public sources:

Credit Information Bureau, Revenue Service, Public Service Development Agency, National Agency of Public Registry, tax service providers, etc. The above information is requested in accordance with the law and, if necessary, based on your prior consent.

When do we share your data with third parties?

The Bank uses data strictly for legitimate purposes.

The data held by the Bank concerning you are strictly confidential and must not be disclosed to any third parties other than those indicated below and to the relevant extent:

- Government/judicial/supervisory/controlling and/or registering state or local self-government bodies, including the National Bank of Georgia, LEPL Financial Monitoring Service of Georgia, LEPL National Agency of Public Registry of Georgia, LEPL Public Service Development Agency of Georgia, LEPL Revenue Service of Georgia, LEPL Service Agency at the Ministry of Internal Affairs of Georgia, etc.

- Credit bureau – the Bank shares your data with JSC Credit Information Bureau Creditinfo Georgia (TIN 204470740) subject to the terms and conditions of a contract with it, the loan contract with you, and as provided by law.
- The Bank founders and their controlling entities.
- Service providers. Besides, personal data are disclosed only to the extent necessary for any particular job/service defined by the contract. Such persons are bound to keep information confidential.
- Your representative/authorised representative

We may need to share your personal data with organisations that are to provide the product or service you have selected:

- If you have our bank plastic cards, we will provide detailed information about your transaction to the companies that help us provide that service (such as, for example, the international payment system operator Visa Inc and MasterCard Incorporated).
- If you take out insurance through JSC ProCredit Bank, we may transfer your personal, bank or commercial data to the insurance company and other reinsurers.
- The above-mentioned service providers are also, for example, Quipu GmbH (a PC transaction processing centre and a Procredit group member); Identomat Inc (a remote identification software provider); payment service providers (including TBC Pay Ltd), etc.

Where we use third-party services as part of our core business, we may need to share your personal data with them to perform specific tasks. Below are examples of cooperation with third-party service providers:

- Legal, audit and other professional services provided by lawyers, notaries, trustees, audit companies, etc.
- Bank contractors who use the Bank's payment services to receive payments from their clients (subscribers) (the so-called billing), including JSC Telasi, Georgian Water and Power LLC, Kaztransgaz-Tbilisi LLC, etc.

In any case, when your data is shared with third parties, we take all measures to ensure data security.

Note that the above list is not complete or exhaustive, and the number of third parties may occasionally increase or decrease. Nevertheless, the Bank will maintain the standard of personal data processing in line with the requirements defined by the Law of Georgia on Personal Data Protection.

How do we manage collected data and ensure their confidentiality/security?

The organisational and technical measures introduced by the Bank ensure the protection of the information we hold from accidental or illegal use, destruction, loss, modification, disclosure, and generation.

We believe data protection is the duty of every employee. Therefore, every year, to raise awareness of proper data protection, JSC Procredit Bank provides training for every employee to discuss the importance of data privacy and customer data protection. Besides, employee access to customer data is limited depending on their activity (the Bank grants access to your data only to the employees who, depending on their activity, need to have access to such data). In addition, every employee is subject to the Code of Conduct that contains personal data protection clauses.

JSC Procredit Bank is subject to the security regulations and standards established by Georgian legislation and adheres to internationally accepted security standards and best practices.

ProCredit Bank does not ensure and is not responsible for the protection of the security/confidentiality of, access to, and contents of the websites that are not the property of the Bank but can be accessed using the links available on our website.

Automated processing of your data

In an automated manner, including through profiling, the Bank is authorised to process your personal data that we possess and/or obtain based on the provisions of the law. This allows us to make prompt, fair, and efficient decisions. Automated decision-making will impact the quality of our current and future products and services. If automated processing of your personal data, including profiling, results in legal, financial, or other significant impacts for you, and this automated processing is not authorized by law, you have the right to not be subjected to decisions made entirely by automated processes, including profiling.

Your personal data is processed to prevent fraud, money laundering, economic sanctions, and financial crime and to identify any related risks. If the Bank identifies a risk of fraud, we reserve the right to temporarily suspend transactions on suspicious accounts and/or refuse to provide relevant services for your own safety.

Processing of data for direct marketing purposes

We process your personal data for direct marketing purposes, which helps us offer banking products and services tailored to your needs. This may include providing information on how to participate in studies, surveys, and promotional draws. Processing personal data for direct marketing purposes is only allowed with your consent.

You have the right to ask us to stop using your personal information for marketing, including sending promotional SMS messages. You won't be charged for withdrawing your consent. We will stop using your data for direct marketing within seven business days

at the latest. You can request this in person at any Bank branch, through Internet or mobile banking, by email, by sending a message to the contact details provided in this document, or by sending an SMS with the word "NO" (see the 'Contact us' section). You may also file a relevant application.

If you are still interested in our banking products or services, even though you previously declined data processing for direct marketing purposes, you can contact us at any time through your preferred channel to renew your consent for data processing for direct marketing purposes.

Please note that the direct marketing provision does not apply to the information provided to the customer regarding its active products. The Bank ensures that the customer is informed of any changes to the product.

Your rights under the Law of Georgia on Personal Data Protection

According to the Law of Georgia on Personal Data Protection, you have the right to request information about the processing of your personal data free of charge. To clarify, 'data' in this context refers to an individual's personal information. Upon request, the Bank is required to provide you with the following information: the specific personal data being processed about you, the purpose of the data processing, the legal basis for the data processing, the methods used to collect the data and how your data is being processed. You also have the right to receive detailed information about the data retention period (time) or the criteria for determining the data retention period, to whom your data has been disclosed, the legal basis and purpose of the data disclosure, information about any automated decisions made, including profiling, or the logic used for such decisions, as well as the potential impact on the processing and the anticipated result of the processing.

You are entitled to request a free copy of the data we hold about you unless:

a) There are specific fees set by the laws of Georgia, or

b) The Bank has set a reasonable fee for providing the data in a different format due to the resources used and/or the frequency of requests.

You have the right to request the correction, update, supplementation, blocking, stopping of processing, restriction of access, deletion, and destruction, as well as the transfer (in the case of automated processing of information) of your personal data if they are found to be false, inaccurate, incomplete, not updated, or if their authenticity/accuracy is disputed, or if their collection and processing is found to be in conflict with the law.

You have the right to withdraw your consent at any time without providing an explanation. You can do so by using the methods specified in the ‘Contact us’ section (such as visiting a branch, using Internet/mobile banking, or sending an e-mail). It's important to note that if you withdraw your consent and there is no other legal basis for processing your data,

the Bank may refuse to provide you with services in full or in part and/or may also terminate any contracts you have with them. This means that after withdrawing your consent, you may not receive the desired level of service or may not be able to access certain services. However, it's essential to understand that withdrawing your consent does not cancel any legal consequences that occurred before the withdrawal. Also, please note that you can revoke your consent free of charge.

The Bank will handle your requests for processing, correcting, updating, completing, terminating, deleting, or destroying personal data within 10 business days, unless the legislation of Georgia establishes a different period or there is another legal basis for processing personal data. In specific cases with proper justification, the Bank may extend this period by up to 10 business days and will promptly notify you. Additionally, you have the right to receive information about the decision to block personal data or the reasons for refusing to block personal data within three working days of the request.

Limitation of the rights of the personal data subject

Your rights may be limited only if it is expressly allowed by the laws of Georgia, do not violate fundamental human rights and freedoms, are necessary and proportional in a democratic society, and if the exercise of these rights puts at risk the values/interests explicitly defined by the law.

Please be aware that we are required to comply with Georgian laws, which may limit our ability to delete personal data immediately. These obligations may stem from anti-money laundering, tax, commercial banking, consumer protection laws, and other legal regulations.

The measure above may only be applied to the extent necessary to achieve the restriction's purpose.

When the law requires it, the Bank will inform you if it decides to restrict or deny your rights as a data subject unless giving you that information would hinder the accomplishment of the goal(s) outlined in the law.

The personal data subject’s right to appeal

If your rights, as outlined in this document, are violated, you have the right to seek assistance from the Personal Data Protection Service, a court, and/or a superior administrative body according to the procedures established by law.

International personal data transfer

The transfer of data to another state and international organization shall be permitted if the data processing requirements outlined in Georgia's legislation are met and if the relevant state or international organization has implemented appropriate safeguards to ensure data protection and the rights of data subjects.

When your personal data is transferred outside the European Union and the European Economic Area, the Bank ensures the security of data transfer and processing in compliance with Georgia's legislation and this document.

International data transfer by the Bank is allowed in the following cases:

- The country with which the information is shared has adequate safeguards for data protection.
- Data transfer is envisaged by an international treaty and the agreements of Georgia.
- Data transfer is provided for by the legislation of Georgia.
- You have given your written consent for data transfer.

Personal data that is transferred to another state or international organization may only be further transferred to a third party if the transfer serves the original purpose for which the data was transferred and meets the necessary conditions and safeguards for data protection as outlined in this Policy.

Personal data retention periods

We will keep the data outlined in this document for the duration of our service to you and for up to 15 years after the service ends, as per the retention terms set by Georgia's legislation.

The reasons for retaining your personal data are as follows: The data is retained in accordance with the law; it is processed and stored to support a claim or statement of defence, to address inquiries and complaints, to safeguard your or the Bank's rights for potential legal proceedings, to preserve evidence, to demonstrate the Bank's compliance with the law, to fulfil obligations arising from transactions with us, to combat fraud and financial crime, and to fulfil other functions and duties assigned to the Bank by law.

Thus, the Bank only maintains information for the period established by law, as defined by internal regulations or required to achieve the purpose of data processing.

Personal data may be retained for longer than 15 years only if relevant legitimate and/or legal grounds exist.

Data protection recommendations

Please note that this Policy may be updated periodically. It is recommended to review it regularly. The latest version of the Policy is available on the Bank's website at www.procreditbank.ge.

To protect your personal data, follow these security measures:

- When logging into our website, use the Bank's internet address (www.procreditbank.ge) in your web browser. You can also access the Internet Banking system by entering https://online.procreditbank.ge in the URL address field

or using the provided link on our website. Only use these methods to access the system.

- Never share your personal or confidential information with strangers over the phone or with third parties. Avoid storing such data in non-password-protected files on your computer, the Internet, or your mobile device.
- Complete any video identification or web application for bank services in person.
- Use your own devices to access our services.
- Provide only your own contact details, such as your mobile phone number and email.
- When conducting online bank transactions, ensure that you are using a secure browser and up-to-date antivirus software.
- Avoid opening email notifications from unknown sources.
- Before logging in to Internet Banking, ensure that you are on a secure ProCredit Bank website at https://online.procreditbank.ge/login.
- Use our online banking product only on your personal computer and refrain from using public Wi-Fi.
- Do not leave your computer unattended after logging in to Internet Banking. Always log out by clicking the logout button when you have finished your session.
- Do not allow the web browser to save Internet Banking or email usernames and passwords for automatic log-in.
- When handling your data, including information from your plastic card, be mindful of your surroundings to prevent access by third parties.
- Do not hand over your plastic card to any serving personnel for making a payment.
- Adhere to any additional actions or recommendations specified by the Bank for each specific service.
- Install and regularly update antivirus software, anti-spy software, and a Firewall on your devices.
- Stay vigilant during online activities and learn to recognize any unusual activity, such as phishing attempts for personal or confidential bank information from new website addresses or emails.
- Note that the Bank will never request confidential information such as passcodes, passwords, card PINs, card PANs, transaction authorisation numbers (TANs), 3D codes, service activation codes, or strong authentication codes via phone call or SMS.
- Disable the autofill function when providing identification and authorization details for services requiring this information (e.g., identification number, phone number, username, password, etc.).

Contact us

To exercise your rights regarding personal data protection, you can contact the Bank's Personal Data Protection Officer, Tamar Asatiani, at any time via email at tamari.asatiani@procredit-group.com or by phone at 598 21 70 31. Additionally, you can visit any branch of the Bank, contact us through the Internet and/or mobile banking, or write to us using the contact information provided below.

We value your opinion. If you have received any suspicious security-related notice or information, please call our Contact Centre at *2222 or (32) 220 22 22 between 09:00 and 21:00. You can also email us at geo.iso@procredit-group.com.