Credo Bank Privacy Policy

ᲙᲠᲔᲓᲝ ᲑᲐᲜᲙᲘ
CREDO BANK

About the Bank:

JSC "Credo Bank" (hereinafter referred to as the "Bank") is a commercial bank licensed under the Georgian legislation.

Identification number of the Bank: 205232238.

Address: 27 R. Tabukashvili str. 0108, Tbilisi, Georgia.

For more information please check here.

Purpose and Scope of this Document:

This Document refers to the policies, procedures and security tools available at the Bank against unsanctioned access to personal information. It covers the data which the Bank obtains when having you as a customer, which is also used for direct marketing purposes in line with the legislation of Georgia. The Document explains the principles we follow while processing your personal data and how the law protects you that is compliant with advanced international best practices including GDPR principles.

This document applies to all data subjects whose data is processed by the Bank, including, but not limited to, bank clients (existing, former, and potential, as well as their official representatives), bank staff members and job applicants, and other data subjects whose data is processed under the Law of Georgia on the Protection of Personal Data.

We, the Bank, promise:

- To keep your data safe and private;
- Not to use your data unlawfully;
- To process your personal data in accordance with the Georgian legislation and best practices, including in compliance with principles of processing set by the Law of Georgia on the Protection of Personal Data;
- That your data is stored in a secure environment and exchanged through secure communication channels in accordance with internationally recognized data security standards and best practices;
- To provide you with complete and exhaustive information with respect to the processing of your personal information.

When processing personal data, the Bank is guided by the following principles:

- Data is processed lawfully, fairly and in a transparent manner in relation to the data subject considering applicable exceptional cases established by the legislation **(lawfulness, fairness and transparency)**;

- Data is collected/obtained for specified, explicit and legitimate purposes. The Bank does not further process the data for other purposes that are incompatible with the initial purposes **(purpose limitation);**

- Data is processed only to the extent necessary to achieve the respective legitimate purpose. The processed data is proportionate to the purpose for which they are processed by the Bank **(data minimization);**

- Data is true, accurate, and, if necessary, kept up to date **(authenticity, accuracy, and up-to-datedness)**.

- Data is stored only for the period necessary to achieve the corresponding legitimate purpose of processing. Once the purpose has been fulfilled, data is deleted, destroyed, or stored in a depersonalized form, unless otherwise required by the applicable legislation and the data storage is necessary and proportionate to protect overriding interests in a democratic society **(retention limitation)**.

- To ensure data security, the bank implements appropriate technical and organizational measures during data processing to protect against unauthorized or unlawful processing, accidental loss, destruction, or damage **(confidentiality, integrity, availability)**.

Legal grounds of processing:

As well as our Privacy Promise, your privacy and personal data is protected by the Law of Georgia on the Protection of Personal Data (the "Law"). Pursuant to the law, the data processing is lawful where one or more of the following grounds exists:

- You have given consent to the processing of data concerning you for one or more specific purposes;
- Data processing is necessary for the performance of a contract of us and you or to enter into a contract at your request;
- Data processing is authorized by law;
- Data processing is necessary for us to perform our statutory duties;
- According to law, the data is publicly available, or you have made them publicly available;
- Data processing is necessary to protect your or another person vital interests;
- Data processing is necessary to perform tasks related to the public interests as defined by the legislation of Georgia;

- Data processing is necessary to protect important legitimate interests of us or a third party, unless there is an overriding interest in protecting the rights of the data subject (including a minor);
- Data processing is necessary to assess an application submitted by you to provide services to you.

The law also stipulates the grounds for processing certain sensitive (special category) data under specific conditions. We only do this when necessary and in accordance with those conditions.

The law also grants you certain rights as a data subject. For more information on these rights, please see the "Your Rights" section.

What types of personal information we process:

We process various types of personal information and classify them as follows:

Type of Personal Data	What specific data might this imply
Identification information	Name, Surname, ID number, signature, date and place of birth, passport details, photograph, identity/nationality details.
Contact data	Legal and actual address, email address, phone number, emergency contact information, postal address
Financial Information	Details regarding financial status, transactions, credit scores and credit history, income details, assets, liabilities, Loan and mortgage information, payment history
Contractual Data	Details on products and services provided to you by us, Information about existing contracts with other financial institutions
Audiovisual data	Recorded telephone conversations with our remote service systems and internal communication systems, visual and audio surveillance footage and images.
Socio-demographic Information	Information on employment, citizenship, education, social status, marital status, family composition

Transactional Data	Account information, information about operations carried out on accounts, products/services, payment history
Locational Data	Location information from your mobile phone, address associated with your internet connection when you access online services and/or data on your purchases using card
Behavioral and Usage Data	Information on how you interact with certain products and services
Data relating to minors	Data relating to minors that are processed on the basis of his/her consent if he/she has reached the age of 16 or with the consent of his/her parent or other legal representative (minors under 16), except cases provided for by law
Data of a deceased person	Bank only processes data of a deceased individual if there is relevant legal ground(s) provided by law.
Technological and technical Data	Information about devices and technology you use (including IP addresses, application logs and log records, cookies, location information, and other related data)
Communication Data	Communications through letters, emails, chats, SMS or other conversations between us.
Documentary Data	Details about you recorded in various types of documents and the copies thereof (e.g., passport, ID card, birth certificate, driving license and other identification documents)
Public Data	Data obtained from publicly available sources
Data processed in accordance with applicable legislation	Data required to be processed under applicable legislation (including but not limited to the requirements under KYC, AML legislation)
Special Categories of Data stipulated by the Law	Considering Law requirements/limitations – Health data, status of an accused, convicted or acquitted person or a victim in criminal proceedings, conviction, criminal record, diversion, recognition as a victim, detention and enforcement of his/her sentence, or his/her biometric and genetic data

Purposes of Processing Personal Data

We process your personal data for the following primary purposes:

1. **To Effectively Manage Relationships With You:**

   We process your personal data to effectively manage our relationship with you, enhance communication, and provide personalized services. This also includes improving customer satisfaction by addressing inquiries and resolving complaints. We also process your data to fulfill our obligations under the contractual agreements and ensure compliance with the terms and conditions. Additionally, we use personal data to send you important correspondence and notifications to keep you informed about updates and relevant information related to your account and services.

2. **To Effectively Meet Your Needs and Preferences:**

   We use your personal data to better understand and meet your needs and preferences, identify new ways for collaboration. This also includes examining how you interact with our products and services to improve our offerings. We also seek expert insights to enhance the quality of our products and services and analyze transaction data, credit history, and other relevant information to continuously advance our banking products and services. Furthermore, we process certain data to evaluate and manage credit risks associated with loan applications and business interactions by reviewing financial, transactional and other data.

3. **To Deliver Our Products and Services:**

   We process your personal data to effectively deliver and manage our banking products and services. This includes handling and overseeing customer payments, managing and processing transaction activities, loan portfolios, and administering client accounts. Additionally, personal data is used for essential activities such as account openings, fund transfers, and transactions as well as providing customer support and ensuring the security of financial transactions. In addition, your personal data may be processed to facilitate investment and wealth management services and deliver digital banking solutions.

4. **To Ensure Business Efficiency, Efficacy, and Effective Governance:**

   We process your personal data to optimize our business operations, ensuring efficiency, compliance, and security. This involves managing financial resources, strategic planning, risk mitigation, reporting, auditing, data security and robust governance. We may also process your data to improve our performance in order to improve your experience and satisfaction with us, also to avoid and effectively manage potential incidents and protect your rights.

5. **Marketing and Brand Management Purposes:**

We may process your personal data to develop and execute effective marketing strategies and activities, enhance our brand, and deliver relevant products and services. This involves conducting market research, analyzing customer preferences, and tailoring our offerings to meet customer needs and preferences (for further details please refer to "Direct Marketing").

6. **To Ensure Effective Risk Management**

   We may process your personal data to manage and mitigate risks (risks associated to us and you) and prevent financial crime. This involves identifying, assessing, and managing financial and operational risks, as well as implementing robust security measures. We may also process the data to conduct ongoing monitoring and reporting to detect and prevent fraud, money laundering, and other illicit activities.

7. **To Ensure Legal and Regulatory Compliance**

   We may process your personal data to comply with applicable laws and regulations. This includes facilitating access to supervisory authorities and auditors as required by law. We also use personal data to meet our legal obligations, ensuring adherence to all relevant legal requirements for proper conduct and accountability. Additionally, your data is used to protect our legitimate rights, which involves handling legal disputes, recovering debts, and safeguarding intellectual property. This encompasses investigating claims, responding to legal issues, and managing legal proceedings.

8. **To Ensure Property and Security Protection**

   We may process your data and use audio-visual, technical, and other data to prevent crime, protect public and personal safety, and ensure the public security and security of our operations.

If the client is a legal entity, if necessary, we process the representative's Personal Data for the purpose of fulfilling the duties imposed by law, protecting the legitimate interests of the bank and/or providing services to the above-mentioned legal entity, as well as providing information/suggestions about direct marketing offers and banking services.

What Could Be Our Legitimate Interests While Processing Your Personal Data:

- Personalizing and enhancing user experience of customers/visitors;

- Ensuring the secure and uninterrupted operation of banking services, the proper and timely execution of clients' requests and instructions, and the proper provision of relevant banking products and services;
- Developing new products/services or improving and offering personalized products to customers;
- Verifying your identity, communicating effectively, and providing personalized service.
- Effective enforcing of our legal and contractual rights;
- To assess our (including our staff) performance to improve your experience and satisfaction with us, avoid and effectively manage potential incidents and protect your rights;
- In case of dispute, effective commencing and responding to legal actions;
- To effectively analyze customer feedback to improve customer satisfaction;
- Ensuring compliance with legal/regulatory requirements and contractual obligations;
- Effective and efficient management of customer inquiries, complaints, and service requests.
- Preventing, detecting, and responding to financial crimes such as fraud, money laundering, and terrorist financing.
- Effective mitigation and management of risks, including operational risks;
- Maintaining accurate and true records and ensuring operational stability;
- Ensuring effective informational security to protect confidential information from loss, unauthorized access or damage;
- Ensuring secure systems and networks to protect Bank's, your and third parties' financial resources and assets;
- Planning effective marketing strategies and conducting marketing activities to enhance customer experience.
- Effective handling of scenarios involving restructuring, acquisitions, or other significant changes.
- Effective handling and responding to incidents, monitoring processes and assessing risks to ensure operational resilience, protecting customer rights during and after incidents.

How the purposes of processing, types of personal data, legitimate interests of the Bank, and legal grounds may align with one another:

How the purposes of processing relate to the types of personal data processed by the Bank:

Purpose of processing	Personal Data Type
Effectively Manage Relationships With Customers	Identification information, Contact Details, Financial Information, Contractual Data, Transactional Data, Communication Data, Behavioral and Usage Data, Socio-demographic Information, Locational Data
Effectively Meet Customer Needs and Preferences	Identification information, Contact Details, Financial Information, Transactional Data, Behavioral and Usage Data, Socio-demographic Information, Technological and Technical Data
Deliver Our Products and Services	Identification information, Contact Details, Financial Information, Contractual Data, Transactional Data, Communication Data, Locational Data, Technological and Technical Data, Special Categories of Data (specifically, biometric)
Ensure Business Efficiency, Efficacy, and Effective Governance	Identification information, Contact Details, Financial Information, Contractual Data, Transactional Data, Communication Data, Technological and technical Data, Documentary Data, Audiovisual Data
Marketing and Brand Management Purposes	Identification information, Contact Details, Financial Information, Behavioral and Usage Data, Socio-demographic Information, Transactional Data, Communication Data
Ensure Effective Risk Management	Identification information, Contact Details, Financial Information, Contractual Data, Transactional Data, Behavioral and Usage Data, Locational Data, Technological Data, Communication Data, Documentary Data, Public Data, Special Categories of Data
Ensure Legal and Regulatory Compliance	All data types
Ensure Property and Security Protection	Identification information, Contact Details, Audiovisual data, Technological Data, Locational Data

How the purposes of processing relate to the Bank's legitimate interests and legal grounds:

Purpose of processing	What legal grounds and legitimate interests the Bank may have in relation to specific processing purposes:
Effectively Manage Relationships With Customers	**Legal grounds:** · Your consent; · Fulfillment of contractual obligations; · Our legitimate interests; · Our legal obligations · Carrying out our core business activities (regarding biometric data) **Legitimate interests:** · Personalizing and enhancing user experience of customers/visitors; · · Developing new products/services or improving and offering personalized products to customers; · Verify your identity, communicate effectively, and provide personalized service. · Effective enforcing of our legal and contractual rights; · To effectively analyze customer feedback to improve customer satisfaction; · Effective and efficient management of customer inquiries, complaints, and service requests. · Maintaining accurate and true records and ensuring operational stability; · Planning effective marketing strategies and conducting marketing activities to enhance customer experience. · To assess our (including our staff) performance to improve your experience and satisfaction with us, avoid and effectively manage potential incidents and protect your rights.
Effectively Meet Customer Needs and Preferences	
Deliver Our Products and Services	
Ensure Business Efficiency, Efficacy, and Effective Governance	
Marketing and Brand Management Purposes	

Ensure Effective Risk Management	**Legal grounds:** · Fulfillment of contractual obligations; · Our legitimate interests; · Our legal obligation. **Legitimate interests:** · Effective enforcing of our legal and contractual rights; · In case of dispute, effective commencing and responding to legal actions; · Ensuring compliance with legal/regulatory requirements and contractual obligations; · Preventing, detecting, and responding to financial crimes such as fraud, money laundering, and terrorist financing. · Effective mitigation and management of risks, including operational risks; · Ensuring effective informational security to protect confidential information from loss, unauthorized access or damage; · Ensuring secure systems and networks to protect Bank's, your and third parties' financial resources and assets; · Effective handling of scenarios involving restructuring, acquisitions, or other significant changes. · Effective handling and responding to incidents, monitoring processes and assessing risks to ensure operational resilience, protecting customer rights during and after incidents.
Ensure Legal and Regulatory Compliance	**Legal grounds:** · Our legitimate interests · Our legal obligations **Legitimate interests:** · Effective enforcing of our legal and contractual rights; · In case of dispute, effective commencing and responding to legal actions; · Ensuring compliance with legal/regulatory requirements and contractual obligations; · Preventing, detecting, and responding to financial crimes such as fraud, money laundering, and terrorist financing.

	· Effective mitigation and management of risks, including operational risks; · Ensuring effective informational security to protect confidential information from loss, unauthorized access or damage; · Ensuring secure systems and networks to protect Bank's, your and third parties' financial resources and assets; · Effective handling of scenarios involving restructuring, acquisitions, or other significant changes. · Effective handling and responding to incidents, monitoring processes and assessing risks to ensure operational resilience, protecting customer rights during and after incidents.
Ensure Property and Security Protection	**Legal grounds:** · Your consent; · Our legitimate interests · Our legal obligations **Legitimate interests:** · Effective enforcing of our legal and contractual rights; · To assess our (including our staff) performance to improve your experience and satisfaction with us, avoid and effectively manage potential incidents and protect your rights; · Effective mitigation and management of risks, including operational risks; · Ensuring effective informational security to protect confidential information from loss, unauthorized access or damage; · Ensuring secure systems and networks to protect Bank's, your and third parties' financial resources and assets; · Effective handling and responding to incidents, monitoring processes and assessing risks to ensure operational resilience, protecting customer rights during and after incidents.

How do we obtain your data?

We obtain your information from the following sources:

- **Directly from you:**

  - Becoming a customer or using our products and services (including online services);
  - Communicating with us (during phone calls, branch visits, sending posts/emails, digital channels (websites, mobile apps, online chat), video calls, social media or other channels);
  - Submitting documents or information to us (such as filling in relevant forms, applications for products or services, inquiring about our products or services, participating in relevant competition or surveys).
  - Performing financial transactions, signing a contract or using open banking;
  - By expressing your consent regarding Direct Marketing.

- **From Third Parties and other sources considering legal grounds, requirements and restrictions:**

  - Third parties (such as, Credit information bureau, supervisory, state and local authorities and legal entities (such as, State Service Development Agency, Revenue Service), other financial institutions, individual entrepreneurs and legal entities, payment service providers and others;
  - Publicly available sources, including business registries, debtors' registries, and other relevant registers.

When the data subject provides the Bank with personal data or other information about a third party, the data subject confirms that they have obtained the necessary consent from the third party and assumes full responsibility for the Bank's processing of such data.

Cookies

We employ Cookies and monitor our visitor behavior on our website to ensure that we provide the best practice to our users while they visit our website and are able to continuously improve the quality of our service. We are gathering information on cookies, visitor navigation and behavior on our digital channels, in particular:

- IP address, type of device, operating system and browser, through which the website is visited;
- Pages opened via our website, session duration and other parameters;
- Information on the actions taken on our website: filling out forms, using interactive elements of the website, etc.
- Process, time and manner of filling out the website fields

We use the obtained information:

- To create and maintain the website statistics for the optimization of processes, fields and website design;
- To protect the website visitors and prevent fraudulent actions;
- To detect and prevent money-laundering, terrorism financing and other criminal activities;
- To assess the control of website visitor flow and marketing campaign;
- Obtained information helps us tailor the website and its components to the needs of the users;
- To establish how our users visit our website.

Before you start the use of our website, you can accept cookies and have your user behavior monitored by clicking the button "approval". If you do not agree with the „Cookie Policy", though you can continue to use our website, this action shall still be considered your approval of the mentioned action.

We are not using the cookie files and the data obtained as a result of monitoring the user behavior for the purpose of gathering the personal information. If you wish to restrict the cookie or block them on our website, you can do it by changing your browser parameters. Besides, please, take it into consideration that some of the services offered by us will not be available if you block or delete the cookie files.

Your rights:

In compliance with the legal requirements and, considering the restrictions and limitations of the Law, you have the right to:

- Request the Bank confirmation as to whether or not data concerning you are being processed and, if requested, receive the details about the data and processing, including but not limited to the information and details regarding who processes the individual's information, by what means, for what period, and what guarantees and protective measures are in place to ensure its security.
- Request access to and obtain copies of your personal data.
- Request from us to correct, update and/or complete false, inaccurate and/or incomplete data to ensure that the data regarding the subject is always accurate, correct, and up to date;
- Request us to terminate the processing of (including profiling), erase or destroy data. The Bank will address your request, but the bank has the right to reject the request if any of the following circumstances exists:
    - There is one of the legal grounds for processing these data;

- Data are processed for the purposes of substantiating a legal claim or a statement of defence;
- Processing of data is necessary for the exercise of the right of freedom of expression or information;
- Data are processed for archiving purposes in the public interest as provided for by law, for scientific or historical research purposes or statistical purposes, and the exercise of the right to the termination of the processing, erasure or destruction of the data would render impossible or substantially impair the achievement of the purposes of the processing.

- Request us to block data if any of the following circumstances exists:
  - the authenticity or accuracy of the data is contested by you;
  - the processing of the data is unlawful, although you oppose the erasure of the data and request their blocking;
  - the data are no longer needed for the purposes of the processing, but they are required by you to lodge a complaint/claim;
  - you request the termination of the processing, erasure or destruction of the data and this request is being considered;
  - There is a need to retain the data for use as evidence.

  The bank will address your request unless blocking the data could jeopardize one of the following:

  - the fulfilment by the controller of the duties assigned to him/her by law and/or a law and a subordinate normative act issued on the basis thereof;
  - the performance of tasks falling within the scope of public interest in accordance with law and the exercise by the controller of the powers conferred on him/her under the legislation of Georgia;
  - the legitimate interests of the controller or a third party, unless there is an overriding interest in protecting the rights of a data subject, in particular a minor;
  - The protection of the vital interests of the data subject or a third party, as well as for purposes related to national security and defense.
- In the case of the automated processing of data in certain cases stipulated by Law and if technically feasible, you have the right to receive data which you have provided to us in a structured, commonly used and machine-readable format, or to require that the data be transmitted to another controller.
- You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or other similarly significant effects, except where a decision based on profiling is:
  - based on your explicit consent;
  - necessary for entering into, or performing, a contract between you and us;
  - Provided for by law or by a subordinate normative act issued within the powers delegated on the basis of the law.
- You have the right to withdraw your consent at any time and without explanation in the same form in which it was given.

- If the rights as provided for and the rules established by this Law are violated, you have the right to apply to the Personal Data Protection Service, to a court and/or a superior administrative body in accordance with procedures established by law.

Please, take into consideration that in accordance of the Law your certain rights might be restricted if explicitly provided for by Georgian legislation, as long as this does not violate fundamental human rights and freedoms, and if it is necessary and proportionate in a democratic society (Please, check the Law on Personal Data Protection[1] for more details and certain conditions).

Please, take into consideration that you may choose not to provide certain personal data to us but please note it may affect our ability to relevant deliver services to you.

To effectively exercise your abovementioned rights, you can use any of the following communication channels:

- Call our call center at: 0322 42 42 42; *4242
- Send us an email at: personaldata@credo.ge;
- Visit a bank service center/branch to address the issue in person or in writing;
- Contact us via our official Facebook page: credo bank / კრედო ბანკი.

Except for the cases and timeframes specifically provided by law, we will respond to your request no later than 10 working days from the date of receipt. In exceptional cases and upon appropriate justification, this period may be extended by no more than 10 additional working days, of which you, as the data subject, will be duly notified. In the case of a request for rectification, updating, completion, suspension, deletion, or destruction of personal data, the response period is 10 working days from the date of the request, unless otherwise provided by Georgian legislation. A request for blocking of personal data shall be executed immediately, but no later than 3 working days from the receipt of the request. In the case of withdrawal of consent, the processing of personal data shall be terminated and/or the processed data shall be deleted or destroyed no later than 10 working days from the date of the request, unless there is another legal basis for processing. Before withdrawing your consent, you have the right to request and receive information about the possible consequences of such withdrawal. If the withdrawal of consent concerns direct marketing, the request shall be executed within a reasonable period, but no later than 7 working days from the receipt of the request.

Regarding direct marketing, the client is entitled to request the bank to stop processing the client's personal data for direct marketing purposes at any time by the following means: By sending NO to 90191, applying the call center *4242/0322424242, and submitting the relevant application to the bank's service center. In such a case, the Bank will stop processing the client's personal data for direct marketing purposes no later than 7 (seven) working days after receiving the request, and the client will no longer receive customized offers.

[1] https://www.matsne.gov.ge/en/document/view/5827307?publication=9

Data processing in mobile banking

When using the mobile banking application, the Bank may process your personal data as defined by the Law of Georgia on Personal Data Protection for the purposes of providing banking products/services/offers, remote identification and verification of a natural person, ensuring the proper and efficient functionality of the application, guaranteeing customer satisfaction, and delivering a service that is as tailored to your needs as possible. This includes processing for analytics purposes. The data that may be processed includes your identification, contact, biometric, location, document-related data, data stored on your device's memory, data uploaded to the application, photos read from the device you use, images taken with the camera, phone contacts, and your music library data (only upon activation by you), as well as identifiers used for advertising and analytics purposes (such as Google Advertising ID, C2DM, App Tracking Transparency) and/or KYC process data necessary for identification, authorization, service improvement, and to ensure the application's functionality. Within the scope of the abovementioned purposes, your identification and biometric data—necessary to verify your identity—may be transferred to the company Identomat Inc., Delaware, USA; Registered office: 8 The Green, STE, A, the City of Dover, County of Kent, Zip Code 19901; Contact: info@identomat.com; Website: identomat.com**.** Additionally, receipts and photos you upload may be processed as part of the "Collect Money" service (if you choose to use this service), for the purpose of classifying your expenses, visualizing them, and organizing your financial data. This data will not be used for automatic decision-making, and the Bank will not transfer this data to third parties.

You can withdraw your consent and/or request the deletion of your data by submitting a request via Mobile Banking. Upon receipt of your request, we will add you to the appropriate list, and your data will not be shared with other applications (for more details please check "your rights").

By registering in the application, you confirm that you voluntarily and willingly provide the mentioned data and consent to its processing solely for the above-listed purpose(s). This consent also serves as the legal basis for the Bank's data processing activities, as defined by law. Please note that the provision of this data and your consent is required in order for us to deliver the relevant services or conclude a contract with you, except for certain elements that you activate optionally within the application. Since these features are enabled at your discretion, the related data is not mandatory to provide. The processed information will be retained by the Bank only for the duration necessary to achieve the purpose of data processing, in accordance with legal requirements and the Bank's internal policies. Regarding biometric data specifically, such data will be generated only during the comparison of the photo taken during the remote identification process with the photo on your identification document. This biometric data will be deleted immediately upon determination of the similarity coefficient (within no more than 10 seconds) in such a way that it cannot be restored. Except for the transfer to Identomat Inc.**,** as mentioned in the first paragraph, and in cases provided by law, no personal data will be transferred to third parties, and no international data transfers will take place.

To learn more about your rights, please refer to the section titled "Your Rights" above.

How we use your information to make automated decisions (profiling)

For making automated decisions, we sometimes use the personal data we have but you have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal or other similarly significant effects, except where a decision based on profiling is:

- Based on your explicit consent;
- Necessary for entering into, or performing, a contract between you and us;
- Provided for by law or by a subordinate normative act issued within the powers delegated on the basis of the law.

This helps us ensure that our decisions are quick, fair and efficient. These automated decisions can affect the quality of products and services offered by us now or to be offered in the future.

Here are the types of automated decision we make:

Pricing

We may decide on the price of some products and services based on the information available to us.

Tailoring products and services to customers' needs

We assign our clients to relevant groups which we call customer segments. We use these groups to study our customers' needs and based on what we learn, make decisions that will be useful and favorable for you. This helps us to design products and services for different customer segments and to manage our relationships with them.

Detecting fraud

We use your personal information to help decide if your accounts can be used for fraud or money laundering. We may detect that an account is being used in a wrongful way. If we identify the risk of fraud, we reserve the right to suspend transactions of doubtful accounts for your security or refuse access to them/deny a respective service.

Opening accounts

When you open an account with us, we check that the product or service is relevant for you, based on the information available to us. We also check that you or your business meets the conditions needed to open the account.

Approving Credit

We use a system to decide whether to approve or not your credit application, whether for a loan or a credit card. This is called credit scoring. It uses past data to predict how you are likely to act while paying back the credit.

Credit scoring uses data from three sources:

- Your application form
- Credit reference agencies
- Data available to us.

Who we share your personal information with (locally and internationally)

We may have to share your personal data in the cases defined by the Georgian legislation or with other companies, which are supposed to provide you with the product or service chosen by you. Here's an overview of the categories of the third parties with whom your information might be shared:

- **For service provision and transactions**, your information may be shared with relevant parties such as authorized representatives, legal entities, and Payment service provider(s), operator(s) of the payment system, remote channels/payment instruments in a contractual relationship with the bank, necessary information (client's personal data) for providing services to the client (including offering various banking/credit product(s), which, in turn, undertake the obligation to protect the confidentiality of the information provided by the bank. Including third parties (who carry out identification/verification of persons in order to provide/render services in accordance with the legislation of Georgia) as well as to the insurance company(s), in order to obtain appropriate insurance services for the client.

- **To comply with legal and regulatory requirements,** we may disclose your data to state authorities, judiciary, regulatory authorities and Law enforcement bodies, as well as other persons who carry out the tasks assigned to the sphere of public interest determined by the legislation of Georgia (including crime prevention, crime investigation, criminal prosecution, administration of justice, etc.) as required by Georgian law or other applicable legislation. This includes fulfilling obligations related to legal compliance, audits, and investigations. Additionally, your personal information may be shared with entities mandated by law, such as credit reporting agencies and organizations responsible for overseeing financial transactions and credit assessments.

- **Regarding credit information and interactions with financial institutions,** we share credit-related data with credit bureaus to support credit evaluations, reporting, and legal compliance. These bureaus may, in turn, share the information with other authorized entities as required by regulations. Additionally, data may be shared with correspondent and intermediary banks, as well as other financial institutions, to facilitate international transactions and related financial operations. In addition the data may be shared with international financial institutions, in order to obtain financing from the bank.

- **Regarding service providers and business partners,** your data may be shared with external IT and cloud service providers, external professionals such as legal advisors, audit companies, and consultants to assist with business operations and ensure compliance with legal requirements. Additionally, to combat and prevent fraud, your data may be shared with relevant specialized fraud detection and prevention agencies. In connection with managing relevant arrangements, including interactions with trustees, investors, and financial advisors and legal professionals. The information may be shared with evaluation companies and any other third parties. In order to offer and provide various services (including evaluation, measurement products/services) to you.

- **In the event of a sale, merger, or restructuring of the bank,** your data may be shared with parties involved in these transactions. These parties will be required to comply with our data protection protocols and confidentiality agreements. Additionally, your data may be transferred to other entities within our corporate group to support service delivery, product development, and operational activities.

- **To the courier companies**, in order to send/deliver the relevant correspondence to you.

- Subject to your consent and in compliance with applicable legislation, **to other third parties.**

- Any foreign state and/or international organizations/services and/or to any company registered in a foreign country for the purpose of providing/improving any banking services to the client, fulfilling the requirements defined by law and/or implementing other legitimate interests of the bank, if there are grounds for Data processing provided by the Law of Georgia "On Personal Data Protection" and in the receiving state and/or international organization/office and/or companies registered in any foreign country, appropriate guarantees of Data protection and protection of Data subject's rights are provided. The transfer of personal data for processing Visa B2B Connect transactions occurs in the United States, where data protection safeguards may not be fully adequate

and consequently, the confidentiality of this data might not be fully ensured. However, the agreement between the Bank and Visa international service Association includes appropriate guarantees, and both parties have implemented the necessary organizational and technical measures to ensure safe data transfer.

Please note that the list provided is not comprehensive, and the number of third parties involved may vary. However, the Bank will uphold the standards of personal data processing in accordance with the requirements of applicable legislation and standards.

Bank may transfer personal data to any third party, if the aforementioned transfer is necessary for the protection of the bank's rights and legal interests, for the assignment of any kind of demand against the client to a third party (including in the process of negotiations with the mentioned third party), for monitoring the fulfilment of the contractual obligations by the client and/or for providing any kind of service/product to the client In order to make an offer and/or provide any kind of information.

Bank may transfer personal data to any third party, for the purpose of providing banking services to the client, monitoring the client or fulfilling the obligation undertaken by the client, for the purposes of fulfilling the obligations undertaken by the contract concluded with the bank, entering into a transaction at the request of the data subject or protecting other legitimate interests of the bank, including, when the bank uses a third party product/service for the purpose of carrying out commercial activities and where the involvement of third parties is necessary for the effective management of the business activities.

Processing Data for Direct Marketing Purposes

We may use your personal information (including through an authorized person(s)) to tell you about relevant products and offers, to form a view on what you may want or need, or what may be of interest to you, provided that you have given your consent for such processing. This is how we decide which products, services and offers may be relevant for you. We can only use your personal data for direct marketing purposes if we have your consent in compliance with applicable legislation. For the purpose of direct marketing, the bank may process the client's identification (name, surname), contact (mobile phone number, e-mail address) and financial Data. In addition, the bank makes direct marketing offers about the bank's products, shares or other marketing offers through the following means:

- by sending a short text message ("SMS") or email;
- through digital channels (ganvadeba.credo.ge, credobank.ge, business.mycredo.ge, mycredo.ge, MYCREDO - Internet and mobile bank for individuals and legal entities);
- through video banking;
- through the call center;
- By the relevant employee of the bank's service center, instalment officer, sales person and village consul.

The consent given by the client shall have no definite term, however, the client shall be entitled to request the bank to stop processing the client's personal data for direct marketing purposes at any time by the following means: By sending NO to 90191, applying the call center *4242/0322424242, and submitting the relevant application to the bank's service center. In such a case, the Bank will stop processing the client's personal data for direct marketing purposes no later than 7 (seven) working days after receiving the request, and the client will no longer receive customized offers. The processing of personal data for direct marketing purposes shall be voluntary. The client's refusal to process personal data for direct marketing purposes shall not affect the bank's provision of services to the client (for further details please refer to "Your rights" above).

Your security and comfort is important to us. Therefore, you will continue to receive service messages regarding the changes in the facilities proposed to you and in terms of service that messages/notifications are not be considered as direct marketing.

Processing of biometric data

Within the certain processes your biometric data may be processed for the purpose of providing banking products/providing services/providing offers and remote identification and verification of a natural person and within the scope of the abovementioned purposes identification and biometric data, that are necessary to identify identity, will be transferred to the company - Identomat Inc, Delaware, USA; Registered office: 8 The Green, STE, A, the City of Dover, County of Kent, Zip Code 19901, contact information - info@identomat.com; website - identomat.com. Personal data may be processed by the Credo Bank only within the scope of the purposes outlined in the present document. By agreeing with this document, you confirm that you voluntarily and willingly provide this information and give your consent to the processing of the personal data only within the scope of the above-mentioned purpose(s), which also constitutes the legal basis for data processing (consent) by the Credo bank. We inform you that providing your data and granting consent are mandatory to deliver the relevant services/ finalize a contract with you. The processed information will be stored by the Bank only for the duration necessary to fulfill the purpose of data processing, in compliance with legal requirements and the Bank's policies. As for biometric data, it will only be generated during the process of comparing the photo of the individual taken during the remote identification process with the photo on the document. The data will be deleted as soon as the similarity coefficient is determined (within no more than 10 seconds) in such a way that it cannot be restored. Except for the transfer of data to the company Identomat Inc., as specified in the first paragraph of this document, and in cases mandated by law, personal data will not be transferred to third parties, nor will there be any international transfer. Except for cases outlined above, including data transfer to Identomat Inc., and instances required by law, personal data will neither be shared with third parties nor subjected to international transfer. For your rights regarding the rights please refer to "Your rights" section above.

Processing of data regarding audio monitoring and video monitoring

The Bank may process data within the scope of audio-video monitoring for the following purposes: prevention and detection of crime, public safety, protection of the safety and property of persons, protection of confidential information, and obtaining evidence in the event of an incident. Sound recording by video cameras takes place only in exceptional cases: to prevent a crime or where there is a threat to life, health or property. The purpose of audio recording in branches and of call-centre calls is to improve quality, record communication with the client and the client's instructions, review complaints objectively and detect fraud. In addition to the above, the legal basis for processing is the Bank's significant legitimate interest, which includes protecting the Bank's property and the safety of its employees and clients, detecting crime and fraud, preserving evidence and recording communication with clients.

Except where such audio-video recording is mandatory, necessary and proportionate and/or where there is no relevant ground established by law, the data subject has the right to refuse it. Unless otherwise provided by law, video recordings are retained for 30 days, VOIX system audio recordings for 3 months, and call-centre call recordings for 15 years, in accordance with the legislation. Recordings are transferred to third parties, namely courts, the prosecutor's office and investigative authorities, only in cases provided for by law, and no international transfer takes place. For the protection of your rights and for matters relating to them, please see the "Your Rights" section above. For any questions or requests, please contact the Personal Data Protection Officer at personaldata@credo.ge.

Processing of data regarding job applicants

The resume you submit may contain personal data that is necessary for Credo Bank to assess your candidacy exclusively for the purpose of establishing a contractual, including employment relationship with you. Providing personal data is mandatory, as without this data, your application cannot be considered. Your personal data will be processed only to the extent necessary for this purpose and will not be shared with third parties. By submitting your resume, you confirm that you are providing this data voluntarily, which constitutes the legal basis for the bank's data processing (consent) as defined by applicable legislation. Your resume may not be considered for the specific vacancy due to the position's requirements or may be retained for consideration for other relevant vacancies. In certain cases, the person authorized to process personal data may be the recruitment platform - Helio AI LLC (identification code: 406404163, legal address: Mikheil Gakhokidze Street, N 54D, Tbilisi, Georgia, contact information - [https://www.helio-ai.com/], which will process the data solely for recruitment purposes and to the necessary extent (Helio.AI's servers, on which the data is stored in accordance with the established procedure, are located in Germany). Submitted resumes may be stored for up to one year. For your rights regarding the rights please refer to "Your rights" section above. For any concerns or questions regarding the protection of personal data, you may contact the Bank's Personal Data Protection Officer at personaldata@credo.ge.

How long do we keep your personal data?

We retain your personal data only for the period necessary to achieve the purpose of data processing, taking into account the storage periods established by the legislation (for the entire duration of the services provided to you and, in addition, for at least 15 years with respect to information related to the client that is stored in electronic form at the Bank) and the Bank's policies.

Amendments to the privacy policy and contact information

We may periodically update this document. The revised version will be published on our website, with the date of the most recent amendment clearly indicated.

For any concerns or questions regarding the protection of personal data, you may contact the Bank's Personal Data Protection Officer at personaldata@credo.ge. You can also talk to our online consultant (www.credobank.ge), call 24 hours a day 7 days a week (+995 32) 242 42 42, contact us through the internet or mobile banking or visit any of our branch.