

Privacy policy of ProCredit Bank (Bulgaria) EAD

Contents

| | |
|---|----|
| 1. Who are we? | 3 |
| 2. Why does the bank collect and use your personal information? | 4 |
| 2.1. To comply with legal obligations:..... | 4 |
| 2.2. To enter into or fulfill contractual obligations: | 5 |
| 2.3. To manage our business for our legitimate interests: | 6 |
| 2.4. Where you have provided consent: | 7 |
| 2.5. When a task of public interest has to be carried out | 8 |
| 3. Basic principles in the processing of personal data | 8 |
| 4. What kind of personal information do we collect? | 8 |
| 5. When and how we collect information about you | 10 |
| 6. How long we keep your personal information | 12 |
| 7. Am I obliged to provide personal data? | 13 |
| 8. How we protect your personal data? | 14 |
| 9. How do we use personal information for direct marketing? | 15 |
| 10. How does the bank make use of Automated Decision Making? | 15 |
| 11. Cookies | 16 |
| 12. Who do we share your personal Information with? | 17 |
| 13. Sending data outside of the EU | 18 |
| 14. Personal Data subject rights | 19 |

This document represents the internal procedure of ProCredit Bank (Bulgaria) EAD for processing personal data. It outlines the Bank's approach to the collection, storage, processing, deletion, destruction and protection of personal data in order to fulfill the requirements of Regulation (EU) No. 2016 / 679 (General Data Protection Regulation). This procedure has been developed in view of one of our main responsibilities as a bank – to guarantee the security of the information entrusted to us and collected by us, as well as its lawful processing under clear rules. This policy provides answers to important questions related to the processing of personal data in the bank, indicating what measures are foreseen and what mechanisms are implemented.

This procedure applies to all our products and services that we offer as a bank and is mandatory for all our employees who, within the scope of their official duties, work with personal data and/or with information that can serve or lead to the identification and recognition of an individual.

Please, take some time to read the Privacy Policy carefully.

1. Who are we?

ProCredit Bank (Bulgaria) EAD is a development-oriented commercial bank, which is entered in the Commercial register and register of non-profit legal entities and the Register of Credit Institutions at the BNB in accordance with the Credit Institutions Law and holds the necessary licenses for the purpose. We provide credit products and banking services to both small and medium-sized enterprises and individuals.

ProCredit Bank (Bulgaria) EAD is registered with the Personal Data Protection Commission as a personal data controller with the following contact details:

Address: Head Office, 26, Todor Aleksandrov Blvd. 1303, Sofia

Tel.: + 359 700 1 70 70 or *7000

Fax: + 359 2 813 51 10

E-mail: contact@procreditbank.bg

ProCredit Bank (Bulgaria) EAD is a member of the ProCredit Group, which is managed by its Frankfurtbased parent company, ProCredit Holding. ProCredit Holding is the sole owner of ProCredit Bank Bulgaria.

Members of ProCredit Group are: ProCredit Holding; ProCredit academies; Quipu (IT consultancy and software development company), ProCredit Bank (Albania), ProCredit Bank (Bosnia and Herzegovina), Banco ProCredit (Ecuador), ProCredit Bank (Georgia), ProCredit Bank (Germany), ProCredit Bank (Kosovo), ProCredit Bank (Macedonia), ProCredit Bank (Moldova), ProCredit Bank (Romania), ProCredit Bank (Serbia), ProCredit Bank (Ukraine), related parties to ProCredit Bank (Bulgaria) EAD.

More information on the activities of the ProCredit Bank (Bulgaria) EAD is available at the official site of the bank: www.procreditbank.bg.

More information on the activities of the ProCredit Group is available at: <https://www.procreditholding.com/>.

2. Why does the bank collect and use your personal information?

The bank gathers, processes and stores information that contains personal data or could be used to identify a person for a variety of reasons and relies on a number of legal bases to use it. We use the provided personal data to develop, prepare and offer you new products and services that meet changing consumer needs and current market trends. We use the provided personal data to process your applications, to help administer your products and services, to ensure we provide you with the best service possible, to prevent unauthorised access to your accounts and to meet our legal and regulatory obligations.

As per Regulation (EU) No. 2016/679 we are allowed to use personal information only if we have one or more of following reasons:

- when it is our legal duty, or
- to fulfil a contract we have with you, or
- when it is in our legitimate interest, or
- when you give consent for it, or
- when the performance of a task of public interest is necessary;

The Regulation (EU) No. 2016/679 treats some categories of sensitive personal information as special, which processing is allowed after your consent. This includes information about racial or ethnic origin, political opinion, sexual orientation, religious beliefs, trade union membership, health data, and criminal records.

The bank receives, processes, stores and protects your personal information under the following reasons:

2.1. To comply with legal obligations:

As a financial institution, our activity is regulated by numerous legal acts and controlled by various supervisory authorities. That's why it is required from us to process and store your personal information, upon compliance with certain legal obligations:

- to verify the personal data provided to us and to identify to meet our legal and compliance obligations, including to prevent money laundering, tax avoidance, financing of terrorism, evading sanctions and fraud under the Anti-money Laundering Law and its Regulations for the Implementation of it, and Measures against Financing of Terrorism Act.
- to report regularly for our activity to the Bulgarian National Bank, as well as to respond to queries raised by the Bulgarian National Bank.

to respond to requests related to Foreign Account Tax Compliance Act (FATCA), to provide data, as stipulated in the Accounting law, Tax-Insurance Procedure Code and other related regulatory framework in line with establishing fair and lawful accounting process;

- to pass data of the ordering party or beneficiary to the receiving or transferring financial institution under the Law on Payment Services and Payment Systems;
- to provide the required information to the Central Credit Register under the Ordinance No. 22 of the BNB;
- to provide reports to the respective authorities related to the prevention of money laundering activities in certain suspicious cases under Anti-money Laundering Law;
- to report/respond to queries raised by regulatory authorities, law enforcement and other government agencies requested for regulatory investigations, proceedings for established inspections within their powers and competences. Such are police, prosecutor's office, court, State Agency for National Security, National Investigation Services, Anti-corruption authority, etc.
- to provide information to private/state judicial enforcers in line with the Civil Procedure Code;
- to provide information to notaries in accordance and under the terms of the Civil Procedure Code;
- to ensure video surveillance under the Ordinance No. 81213-444 of the Ministry of Interior and the BNB for organization and Control over Ensuring Security of Banks and Non-bank Financial Institutions on the premises, such as in the Bank's offices;
- to provide information that contains or could contain personal data, in line with the internal exchange of information within ProCredit Group in order to comply with legal obligations that the ultimate parent of the ProCredit Group is subject to internal audit and assessments, internal oversight and reporting, including anti-money laundering, and prevention of financial fraud and evasion of sanctions at the group level.

2.2. To enter into or fulfill contractual obligations:

Upon entering and/or fulfilling contractual relationship with the Bank under the pre-contractual and / or contractual relationship, the Bank must take steps that are necessary to provide and/or secure the agreed credit product or banking service, respectively shall have the right:

- to collect, process, store personal data in order to identify you in the verification and processing of a request for the provision of selected and requested applications for products and services in order to assess the terms upon which we can enter into the contract with you.
- to process and store your personal information for the purpose to manage and administration of the occurred upon contractual relation with us legal relationship: your payment/ fiduciary accounts and / or other accounts or services, loans, letters of credit bank guarantees and any other credit products or services.

- To assess the changes in your creditworthiness and collect additional information from its internal systems and databases, as well as from public registers, such as Credit register, Trade register, Bulstat register, Property register, the system of The National Insurance Institute, CRSP, etc.
- To execute ordered transactions and to process payments that are paid to you or by you.
- To contact you by post, phone, text message, email, social media, fax, using our online banking platform – ProB@nking, mobile application or other means, but not in a way contrary to law.
- To provide information about the products and services you use, by sending you notifications, error or incompleteness reports or responses to your requests, questions, complaints or appeals, as well as to inform you about the current conditions for the use of products and services, as well as about changes that have occurred, if any.
- As part of the fulfilment of our contractual relations to you, we may pass some personal information to an intermediary or counterparty (experts in certain service and/or subcontractors) with aim to provide you with the best service (e.g. in case of encashment services).

2.3. To manage our business for our legitimate interests:

The legitimate interests upon which the Bank processes the personal data you provide to us, are mainly:

- In order to determine the most suitable product or service that will fulfill your expectations and will correspond with your repayment capacity, we might collect additional information about you and the other parties related from public registries such as Central Credit Register, Property register, Bulstat register, State fund agriculture register, Central Register of Special Pledges, Trade register, etc.
- In order to be able to provide you with high quality and timely services we share your information with other organisations – cash management companies, legal advisors, notaries, insurance companies, appraisal companies or other third party service providers;
- In order to fulfil internally-set administrative goals, the bank might provide your personal data to archiving companies, debt collection companies and/or members of ProCredit Group;
- When analyzing the internal rules and procedures of the Bank, with the aim of improvement and optimization;
- To record conversations when you contact us via our call center with aim to provide quality service;
- To contact you for marketing purposes in case you are our client, in order to inform and offer you new banking services;
- To carry out various market studies, with the aim of developing new and/or improving existing credit products and services;

- To use and process, your personal data when exercising and safeguarding our rights, including where necessary to take enforcement action (e.g. debt collection);
- To set up video surveillance not stipulated by law, e.g. at the 24/7 self-service zones or inside premises for the prevention of crime or fraud;
- To ensure the physical safety of the Bank's employees and customers who have visited physical sites of the Bank;
- To carry out internal investigations and inspections of various criminal acts and events, in order to provide evidence to a competent supervisory authority;
- To process the submitted complaints and signals from customers, as well as to carry out the relevant internal checks;
- To ensure the security, incessancy and continuity of business processes and activities;
- To ensure strict risk management;

2.4. Where you have provided consent:

The Bank processes and stores your personal data after your explicit consent in the following cases:

- To access personal data from Social insurance register, after submitting application for using a product, offered by the Bank;
- To use your information for direct marketing before you become our client.
- To collect sensitive information – for your health or other sensitive information which you share with us while applying for a product or service or when requesting a change to an existing product and service;

Consent must be freely given by a clear, specific and unambiguous statement. It can only be given through an active action such as a written or oral declaration, or electronically by checking the relevant box, pressing a function button to go to the next page or the next step of a process, and/or selecting and changing the technical service usage settings. Express, clear, specific, unambiguous and freely given consent is also considered the overall behavior of the user, which clearly shows that the user agrees to the provision and processing of personal data and/or information that can lead to his identification.

You can withdraw the consent at any time through our official contact channels in a way that allows your indisputable identification, free of charge. In this case the bank will not use your data for the purposes described above. The withdrawal of consent might reflect into provision of our services or products.

2.5. When a task of public interest has to be carried out

This includes all cases where we are obliged by a supervisory and/or investigative body to provide active assistance to it in an inspection or investigation initiated by it within its competence and accordingly it has requested our active participation or we have obliged by assigning us a task related to with the detection, detection or prevention of crimes.

3. Basic principles in the processing of personal data

This policy for processing personal data has been developed taking into account the following principles:

Legality, good faith, transparency

Internal rules and organization of processes and systems are created to ensure that personal data is processed legally, fairly and transparently, without limiting the rights of customers, employees, job applicants, as well as suppliers who provide various products and services for our business. Any processing that can be attributed to any of the grounds comprehensively listed in point 2 of this procedure is considered lawful and in good faith.

Principle of limitation of objectives

ProCredit Bank (Bulgaria) EAD collects personal data only when it is necessary to achieve specific, explicitly and previously stated, lawful goals. The collected personal data and/or information that can lead to the identification of a person is not processed in an additional way that is beyond the limits of the previously announced goals and/or incompatible with them.

Data minimization principle

In our activity, when working with personal data, we adhere to the legally stipulated minimum as a necessary volume of provided data and information. We do not set additional requirements. In the event that this is necessary, for example in order to provide a service, the customer is expressly informed of this and given an explanation as to why it is necessary to provide additional information.

Principle of data accuracy

The Bank takes all appropriate and proportionate steps, relating to technological development, credit products and services offered, to ensure that all provided and processed personal data are up-to-date and inaccurate data is deleted or corrected;

4. What kind of personal information do we collect?

The Bank collects, records, structures, organizes, processes, stores, if necessary updates personally or through its agent or through our alternative channels of communication such as internet banking Prob@nking or our website different types of personal data from our clients (potential and current) in the context of creating / developing business relationships. The information we process, structure,

analyze, and store may vary depending on the products and services the customer uses. It falls into various categories, as listed below:

- **Identity and contact information**

Name, gender, date of birth, place of birth, copies of identification card or other identification document such as driving licence, passport (personal identification number/foreigner identification number, document type, document number, issuing authority, issue date, expiration date), nationality, photograph, address (country, country region, zip-code, city, street address), contact information (personal email address, home and/or mobile telephone numbers, work phone number, work email address), marital status, family details, professional experience, education, tax residency and tax related information, authentication data (specimen signature);

- **Financial details/circumstances**

Financial status and income details, processing of application and accompanying documentation, employment status and employment of the related persons, credit history, credit assessment records, data from public registers, , financial needs, relationship with other banks or financial companies, business records of self-employed individuals, property documentation collateral information, (property description, data for Properties register, property valuation report, collateral insurance, construction documentation, ownership of movable or immovable assets);

- **Information, related to bank's products and services**

Data from the fulfilment of our contractual obligations, data in the documentation, bank account details, credit/debit card details, transaction details and history, data, related to power of attorney arrangements, information on any third-party beneficiaries; details of products held and applied for including reasons for not proceeding where relevant, other data about the use of the bank's products and services; internal client ID, internal product or collateral IDs;

- **Technical information and online identification**

Information: about the electronic communication and user identities - user login and subscription data (e.g. login credentials for online banking); location details from mobile or other devices, unique identifier for your device, IP address of the device, from which are accessed the banking services, details on the devices and technology you use, log history, data for merchants where you pay with your card; and data about "cookies", used by our internet sites;

- **Information you provide us about others/ related party or others provide about you**

In case you give us information about someone else (for example, data about a spouse or financial associate during the course of a joint application with that person), or someone gives us information about you, we may add it to any personal information we already hold and we will use it in the ways described in this Data Privacy Notice. A financial relationship may be created between the records of persons with economical or kinship relations.

A person or legal entity may disclose information about other persons, only in the cases they have assured the third parties' consent to do so and may provide a proof for their consent to the Bank. The

person or legal entity bears responsibility to provide data in line with the Data Privacy Notice of the bank and the legislation, related to personal data protection.

- **Sensitive categories of data**

Upon a presence of your consent and/or if we have a legal obligation, we may process and store information about you which includes sensitive personal data, such as health or criminal conviction information. We will only hold this data when we need for the purposes and retention periods of the product or services we provide to you.

We collect personal data in relation to children only in compliance with the legal requirements and after having obtained the explicit consent their parents' or legal guardian.

- **Other types of personal data**

Images from security cameras in and around the bank's premises and 24/7 self-service zones; voice from telephone recordings; complaints and information in relation to execution of data subject rights; records of correspondence and other communications with the bank; investigations data (e.g. sanctions and anti-money laundering checks, external intelligence reports);

- **Information about non-clients**

The Bank processes data about parties, related to transactions; data about guarantors; collateral owners; cardholders; authorized persons or clients' representatives by law or with powers of attorney; persons, applying for bank's products and services; data about former clients held till the lawful retention periods; persons in the scope of authorities' investigations; service providers or their employees; images of visitors in premises, held in the lawful retention periods;

5. When and how we collect information about you

This section lists the places where we collect data and information that counts as part of your personal information.

The bank processes data that is initially provided by you, in order to conclude a contract for a credit product and/or service. This is information that you voluntarily provide to us during the process of applying for credit products or using banking services and, accordingly, creating the necessary user profile in our system - by registering in the relevant technological platforms that are provided for the purpose. At this stage, a number of legal obligations are laid down, which require us to clearly and unequivocally identify you and to carry out various checks to determine the type of service and the way in which you can use it.

During the application process, Pre-Contractual Relationships are created where no contract has yet been concluded, but communication and information are exchanged, which are freely provided and in turn necessary to meet the requirements for the conclusion of a contract.

Furthermore, ProCredit Bank (Bulgaria) EAD collects information that contains personal data and allows the identification of a user within the framework of already established contractual relations. This information is collected on the one hand in view of its technological nature, i.e. is generated in the course of using the agreed and provided credit product and/or service. These are all situations in which transactions are carried out, payments are made, credit installments are made, credit is restructured, or communication is conducted with you as our customer via your preferred communication channel. Within the framework of established contractual relations and the use of a provided credit product and/or banking service, information containing personal data is generated and collected when changes are initiated by you. This also includes the situations in which we carry out ongoing control and checks on how the agreed credit products and services are used, in order to fulfill our legal obligations to supervisory and control authorities.

Information that contains your personal data can be used for your initial identification when applying for a credit product and/or service:

- When you apply for products and services of the Bank in our office and submit an application on paper and submit the necessary documents for opening an account, deposit or apply for a credit product;
- When you browse the Bank's website through your electronic device;
- When you visit our offices and/or 24/7 self-service areas of the Bank and use on-site services;
- When you use the Bank's online banking platform - ProB@nking and/or our mobile banking application;
- When you apply for products and services of the Bank through our website, using your device;
- When you provide us with information verbally - during a telephone conversation, with an employee of our Customer Service Center;
- When using the "Bank alone" option, in which a Video connection with our employee takes place;
- When you provide us with information in writing - either by letter on paper by courier, by Application submitted on paper by our employee in an office, or by e-mail when you notify us of any circumstance related to the use of a product or service and /or attach documents;
- When financial analysis and assessment of creditworthiness is made;
- When monitoring is carried out in order to verify and analyze how contractual obligations are fulfilled and how the agreed service is used;
- When you use our products or services, we collect details of how and from where you access them, as well as a history of their use, which we systematize and upload to your profile so that it is available for your reference;
- We use CCTV to monitor offices and 24/7 time zones for self-service and image collection.
- When you visit and view the Bank's social media profiles, such as Facebook, LinkedIn, Instagram or view the Bank's official YouTube channel;

The Bank may also collect, process, classify and store personal data that it lawfully receives from legal entities, individuals or other sources:

- Information that is freely accessible and publicly available - publications and reports in the media, including specialized publications, Company websites, social networks - personal and company user profiles and YouTube channels, trade directories and databases;
- Information from public registers - Commercial Register, Central Credit Register, Property Register, Agency for Geodesy, Cadastre and Cartography, State Fund "Agriculture", National Insurance Institute, National Revenue Agency, Internet portal of the police for checking the validity of identity cards, etc.;
- Information from socially or economically related persons, such as employers, business owners, partners and co-owners, relatives or other persons;
- Information from state authorities and law enforcement authorities;
- Information from credit card providers such as Visa and Mastercard or transaction networks;
- Information provided by customers and business partners of the Bank, within the framework of already established relations for the use of services and products within their scope of activity, such as merchants using POS devices, performing SWIFT and SEPA transfers and transactions and/ or accepting online payments;
- Information from insurers, recruitment agencies.

6. How long we keep your personal information

How long the personal information is stored depends on the nature of the information we hold and the purposes for which it is processed. ProCredit Bank (Bulgaria) EAD determines appropriate retention periods having regard to any statutory obligations imposed by law.

We will process your personal data as an administrator of personal data for as long as we have a business relationship with you - as an individual or in respect of our relationship with a legal entity you are authorized to represent or are owner. After termination of business relationship with the Bank the personal information is kept according to the legal safe-keeping and documentation obligations based on the Anti-money laundering act, the Law on Credit Institutions, Law on Payment Services and Payment Systems, Ordinances issued by the BNB, the Commercial Act, Accounting law, Tax-Insurance Procedure Code, etc.

For example, the account information will be stored for 6 years from the date of account closure. Where you hold or are associated to multiple accounts (including any deposit accounts), the 6 years is effective from the date of closure of the last account.

Information about loans will be stored for 5 years from the date of loan repayment.

We have a strict retention period for security cameras images. In certain limited circumstances, the recordings may be kept for longer, for instance, to provide evidence to the public authorities for investigations for fraud purposes or criminal proceedings.

If the purpose for which the information was obtained has ceased and the personal information is no longer required, the personal information will be deleted. In the events where the reason for which the information is processed has ended, but the collected information is still needed, the personal data

is removed, i.e. all identifying characteristics are deleted, but the information itself continues to be processed. This anonymized information is processed primarily for statistical purposes, for various internal checks that are not related to criminal acts and for marketing purposes when market research is carried out for the purpose of developing new credit products and/or modifying existing ones products and services.

If you would like further information about our data retention practices, contact our DPO using the contact details in this Privacy Notice.

When you have applied for the use of a banking service and/or credit product and within the framework of this application you have provided information that contains personal data in order to be identified, but you have subsequently changed your decision - you have decided that you do not wish to use the relevant service or product, or you have not been approved, the personal data that has been provided is deleted immediately in view of the fact that none of the grounds for processing are available. In these cases, the personal data are immediately deleted and stored in this anonymized form for the needs of statistical processing, reporting and the development of new credit products and services.

Each of our clients, after termination and/or completion of their contractual relationship with the Bank, can benefit from the "right to be forgotten". For this purpose, an application in free text must be sent through one of the possible communication channels, from which it is clearly and unequivocally understood what his request is. After which the Bank, in its capacity as a personal data administrator, will process the application and in the event that there is no reason related to the performance of a task related to the protection of public interest, for example, they are not used by a supervisory authority within the framework of an inspection initiated by it, the personal data will be immediately deleted from all possible records and storage systems.

7. Am I obliged to provide personal data?

Every single aspect of the banking activity is strictly regulated by various control and supervisory authorities that operate at the national and international level. They monitor the strict application of stipulated norms. That's why in the context of the business relationship with the bank, you must provide personal data which is necessary to establish and maintain the respective business relationship, as well as data which the bank is required to collect on the base of local and EU legislation. At any moment, the Bank must know who is the user of a banking service or credit product and on what basis. Respectively, to be able to identify the user of the respective service or product. This is also necessary regarding the protection of your interests as users of banking services and credit products.

You can choose not to give or share with us personal information. Kindly note that if you do not provide us with the required data, then we will not be allowed to commence or continue our business relationship either to you as an individual or as the authorized representative or beneficial owner of a legal entity. On the other hand, at any moment you can freely withdraw your consent to the processing and storage of your personal data in relation to a specific process, service or product. But in these cases, it is possible that access to the respective product will be limited or even denied, as well as the

functionality that was used at that moment will no longer be available. This mainly applies to online banking through the ProB@nking platform and mobile application.

Sometimes the requested by us information is not required by law or a contract, but it is important for us, for example when examining market needs with intention to offer you a new banking service. The collection of such information will be processed only in case of given consent. If you do not give us these extra details, it will not affect the products or services you have with us.

8. How we protect your personal data?

We use a range of measures to keep information safe and secure, as we apply the all technical and organizational measures required by the Personal Data Protection Act, and best banking practices and bank-related legislation. The bank has assured structures for information security and data protection such as Data Protection Officer and Data Protection Committee, as well as Information security and IT security specialists.

The necessary hardware and technical devices are put into operation, which aim to protect and increase the security levels of the corporate network. Various software products and tools are installed, which aim to ensure monitoring of activities in the corporate network, as well as to secure the application of the classic Confidentiality-Integrity-Availability triad, in relation to information, and in particular about information that contains personal data. A system of access permissions has been developed for employees, in view of their official powers, rights and obligations, following the "Need to Know" rule. Thus, no employee has complete and independent access to all customer information databases, and a limited number of employees have the right to make changes to recorded and stored information.

A data encryption and pseudonymization system has been established. An internal convention and system of codes has been developed, which is used in the naming and introduction of the contracts for the various credit products and services in the system. The key for deciphering pseudonyms and service codes is kept separately and access to a specific employee is given after the notification and approval of the head of his department. Each department uses a separate key, so no single employee is able to perform a full and comprehensive identification of a customer in relation to all the credit products and banking and other services he uses, and can recognize and use only the information that falls into his official powers.

In order to minimize the risks associated with the loss of information due to technical failure or interrupted access, several independent information repositories have been built, which are periodically synchronized with the main banking system.

Every new employee, upon joining ProCredit Bank (Bulgaria) EAD, undergoes initial training on personal data issues and is thoroughly familiarized with the privacy policy and the personal data processing policy. We conduct periodic trainings - at least once a year - on issues of personal data protection. These trainings are mandatory for all employees and they explain the key points in the protection and processing of personal data and information that can lead to the identification of a person, as well as the related risks. Depending on their role and functions in the Bank, some employees undergo additional training on the subject.

We require our staff and any third parties, which process your data, to comply with high data protection standards including obligations to protect any information and apply appropriate measures for the use and transfer of information, or on another previously indicated by you preferred channel of communication.

We have established data retention policy and data breach procedure.

9. How do we use personal information for direct marketing?

The bank may process your personal data or data, related to individuals connected to your business to provide information about products, services and offers that may be of interest to you or your business. We may send marketing messages by post, email, telephone or text messages, or by another previously indicated by you preferred channel of communication.

The personal data that we process for this purpose, consists of information you provide to us and data we collect and/or infer when you use our services. We can only use your personal data to promote our products and services to you if we have your explicit consent to do so or, when you are our client under legitimate interest.

You have the right to object at any time to the processing of your personal data for marketing purposes, by contacting the bank and requesting the termination of the use of your personal data for these purposes. In case you request not to send marketing messages, the bank will continue to use contact details to provide important information, related to our contractual obligation with you. We also inform you that the processing of your personal data will be lawful if the Bank has processed the same on the basis of your express consent before it is withdrawn.

10. How does the bank make use of Automated Decision Making?

The bank does not use automated decision making and profiling as the main, independent and leading method in the process of establishing business relations with you and the related checks.

Individual phases and stages of the Bank's processes and procedures are automated, where the application of automation is strictly limited. Stages related to the processing of a large amount of uniform and standardized information are automated, and the results obtained are then subject to verification and assessment by an employee of the Bank.

The bank does not use fully automated processes. The automation is done in order to facilitate and assist the Bank employee in making the final decision. This is one of the tools he uses in making his decision. The decision is made by an employee who has the necessary qualifications, has undergone internal training and is familiar with the rules, practices and standards of the Bank's work, and not by a software algorithm for automated decision-making.

In connection with our legal obligations to prevent money laundering, fraud and the prevention of terrorist financing, the Bank may use automated processing and profiling to verify suspicious

transactions or to identify payments that may be subject to international sanctions. Identified suspicious transactions are subsequently checked manually by Bank employees.

11. Cookies

ProCredit Bank Bulgaria is using “cookies”.

A "cookie" is a small text file that our web server sends to your device - computer, laptop, tablet or smartphone. This file is stored in the corresponding folder for cookies, made by your browser on your computer. The main function of the "cookie" is to allow our webserver to partially recognize your operating system and Internet browser settings in order to improve and optimize the performance of our website. Another important goal of the cookie is to provide feedback on the performance of our site and to gather statistics to help us choose and improve the services we offer.

Some cookies are important to the site's functionality and are automatically activated when visited by users.

Types of cookies that are used by ProCredit Bank Bulgaria:

On the Bank's Internet banking website (<https://probanking.procreditbank.bg/>), the cookies are:

- *PRCBAUTHENTICATIONBG* - a cookie that is a functional necessity. This cookie is used to authenticate and authorize users.
- The cookie is deleted when you exit the system. In memory cookie.
- *PRCBLOCAL* - a cookie that is used only to track the language the client uses (Bulgarian or English). It is not deleted when you exit the system. Temporary cookie.
- *ProCreditBG_AntiForgeryToken* - Security cookie. It is not deleted when you exit the system. In memory cookie
- *_ProAJXSM* - a cookie that we use only as an aid, which contains text (related to the success / failure of the request). Deleted as soon as it arrives at the customer. In memory cookie.
- *fileDownloadToken* - the temporary cookie we use when attempting to download a file from the system (for example, a payment order as PDF). There is a temporary nature, which means that as soon as we have finished working to determine whether the client has downloaded the cookie file is deleted (marked as Expired).
- *PIWIK cookies*. PIWIK is a system that tracks and collects statistical information about the operating system, browser, language, and geographic location of users visiting the site. Used for analyzes and statistics related to the use of our site.

On the Bank's internet page (www.procreditbank.bg), the cookies are:

- `__utm.gif` - Google Analytics Tracking Code that logs details about the visitor's browser and computer.
- `__utma` - a "cookie" that collects data on the number of times a user has visited the web site as well as dates for the first and most recent visit. Used by Google Analytics.
- `__utmb` - Registers a timestamp with the exact time of when the user accessed the web site. Used by Google Analytics to calculate the duration of a web site visit.
- `__utmc` - Cookie purpose description: Registers a timestamp with the exact time of when the user leaves the web site. Used by Google Analytics to calculate the duration of a web site visit.
- `__utmz` - Collects data on where the user came from, what search engine was used, what link was clicked and what search term was used. Used by Google Analytics.
- `_ga` - Registers a unique ID that is used to generate statistical data on how the visitor uses the web site.
- `_gat` - Used by Google Analytics to throttle request rate.
- `_gid` - Registers a unique ID that is used to generate statistical data on how the visitor uses the web site.
- `_pk_id#` - Collects anonymous statistics on the user's visits to the web site, such as the number of visits, average time spent on the web site and what pages have been read.
- `_pk_ses#` - Used by Piwik Analytics Platform to track page requests from the visitor during the session.

You can block or restrict cookies set by any website, including ProCredit Bank sites, through the browser settings of each browser you use on each device you use to access the Internet.

Please note that some of our services, such as Internet Banking, will not work if your browser does not support cookies.

12. Who do we share your personal Information with?

Within ProCredit Bank (Bulgaria) EAD your data is received by the employees of the respective departments that need to process the information in fulfilment of their duties. As a rule, ProCredit Bank (Bulgaria) does not share or send your personal data and the respective information to outside organisations and third parties. But there are certain situations when ProCredit Bank (Bulgaria) might share your personal information with outside organization. Firstly, for fulfilling our contractual or regulatory obligations or for improving the quality of bank's services. We only share your information with a limited number of individuals and companies, which have entered into contractual agreements with the bank, thus observing confidentiality and data protection according to the data protection law and Regulation (EU) № 2016/679.

We only permit service providers to use your information in accordance with our instructions, and we ensure that they have appropriate measures in place to protect your information and apply the same strict standards for processing information that contains personal data that we adhere to.

Sharing can occur in the following circumstances and/or with the recipients, for example:

- **Authorities** to which we have a public or legal duty to share information: Supervisory and other regulatory and public authorities. Examples are central and local government, the Bulgarian National Bank, Revenue & Customs agencies, Deposit Guarantee Scheme, Law enforcement and fraud prevention agencies; Anti-corruption authority, Commission for Personal Data Protection, CRSP, NII, etc.
- **Your authorized representatives:** anyone who provides instructions or operates any of your accounts, products or services on your behalf (e.g. Power of Attorney, solicitors, intermediaries, joint account holders, co-debtors, guarantors etc.) and anybody else that we have been instructed to share your information with by you and has legitimized himself according to the relevant legal order that he has the right of access and the right to use this information;
- **Third parties we need to share your information with in order to facilitate payments:** for example, Visa, Mastercard, credit card issuers and merchant banks, correspondent banks, ATM administrators, Card payment processing companies, your beneficiaries, SWIFT, SEPA, clearing or settlement systems;
- **Other credit or financial institutions:** ProCredit Group members; credit and financial institutions, providing funding to you, for example the European Investment Fund.
- **Companies that provide services for the purposes of fulfilling our legitimate interests or contractual obligations:** for example cash management companies, external legal advisors, notaries, property appraisal companies, insurers, auditors, accountants, marketing and advertising companies, document storage, archiving and destruction companies, cloud storage companies, IT and telecommunication service providers, software development contractors, computer maintenance contractors, printing companies, debt collection agencies, consultants, private/state judicial enforcers etc.

Please note that all the above recipients process your data exclusively for the purposes for which they were collected. The processing takes place after signing a confidentiality agreement and explicit confirmation by the provider of the relevant service that he is familiar with and accepts the Personal Data Processing Policy of ProCredit Bank (Bulgaria) EAD, undertaking to ensure at least the same level of protection and confidentiality and, in turn, has committed and implemented measures for the processing and protection of personal data and/or information that can be used to identify a person.

13. Sending data outside of the EU

Your information and information relating to individuals connected to your business may be transferred to and stored in locations outside the European Union (EU), including countries that may have lower level of protection for personal information. When we do this, we ensure the company that receives the personal data has an appropriate level of protection. Information is requested and checks

are carried out to establish whether it has the necessary technological means and resources, has employees who are prepared and trained to work according to the requirements and standards of Regulation 2016 / 679, has developed policies and procedures for the processing of personal data and information that contains such data, has developed similar mechanisms to those applied by ProCredit Bank (Bulgaria) EAD for the storage and protection of personal data against destruction or unauthorized access. Only then a contract is drawn up, in which the rights and obligations related to the conditions and parameters of the transfer are clearly spelled out. After successfully passing the series of checks and concluding a contract, it is assumed that the transfer is legal. We may need to transfer information in this way to carry out our contract with you, to fulfil a legal obligation, and for your or our legitimate interests.

We may transfer or allow the transfer of information about you and your products and services with us to our service providers and ProCredit Group outside the European Union , but only if they agree to act solely on our instructions and protect your information to the same standard that applies in the European Union.

More information you can find on the European Commission web site following the link here:

https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu_en

14. Personal Data subject rights

Under the GDPR all individuals have the following rights:

- To receive information access to their processed personal data;

Any individual, at any moment, through any of the available and accessible communication channels, can make a request to ProCredit Bank (Bulgaria) EAD whether personal data about him or her is being processed and stored. If there are any, it is permissible to request information about exactly what personal data is processed and stored, for what purpose, what is the source of this information, as well as with whom and under what circumstances this information could be shared. The request can be made in free text, no special form is provided for it. What is important is that it contains enough information to allow the individual making the request to be identified and to be clear about exactly what the request consists of.

- To request incorrect, inaccurate or incomplete personal data to be corrected;

This right can be exercised at any time after the inconsistency or incompleteness in the personal data stored about him is established.

- To request to "be forgotten"- to ask their personal data to be deleted when it is no longer needed or if their processing is illegal;

When a person takes advantage of his right "to be forgotten", this obliges the controller of personal data to destroy all records and all available information about him, on all media and all copies, in the shortest possible time in view of the accumulated information .

- To receive their personal data in a machine readable format and send them to another administrator ("data portability");

The individual has the right to request at any time from the administrator a copy of the information collected and processed about him, which contains personal data and can be used to identify him. This copy should be provided free of charge as soon as possible in view of the information accumulated to date. The copy must be able to be processed without the need for specialized hardware and/or software, i.e. be in a popular and recognizable format. It is preferable that the copy of the information is structured as simply as possible. When there is a large amount of accumulated information about the individual and neither the requirement of short periods nor the requirement of a simple form that allows quick and easy understanding can be met, then the administrator is free to select and filter the available information so as to provide the individual, a clear and detailed representative sample to allow him to navigate what has been collected, processed and stored as personal data and information about him.

- To object processing of their personal data for marketing purposes or when related to a particular situation;

The private person can object by explicitly expressing his/her disapproval of specific personal data being used for specific purposes and/or in specific situations and/or specific methods. An objection can be very narrow in scope, but it can also be very broad and circumstantial and affect a small or large amount of data.

- To request decisions based on automated processing that affect them and based on personal data be made by individuals, not just computers.

It has already been said that any individual can ask the administrator for information on what personal data is being processed, how it was collected, for what purpose, with what methods it is being processed. This right has its natural extension and covers situations in which automated means and tools are used for personal data processing and decision-making, such as some form of artificial intelligence. The private person has the right to contest a decision made by this automated system and to request a natural person, i.e. officer of the administrator to review his case and make a decision. This is because life situations are complex and too diverse to be put into algorithms, i.e. computer logic cannot be applied to them, which only two positions - 1 and 0, i.e. true / false.

ProCredit Bank (Bulgaria) EAD, in its capacity as a personal data controller, must comply with the rights granted to private persons and develop mechanisms for their free exercise, as well as technologically ensure their free exercise.

Individuals can exercise their rights by contacting us using the contact details of the bank:

Address: Head Office, 26, Todor Aleksandrov Blvd. 1303, Sofia

Tel.: + 359 700 1 70 70 or *7000 dpo@procreditbank.bg

For permission to access and correct your personal data or any other requests related to your data subject rights, please submit an application at any of the Bank's offices or use the online banking facility, which allows your personal identification.

You also have a right to complain to the Bulgarian Data Protection Commission . **Commission for Personal Data Protection**

2 Tsvetan Lazarov Blvd.

Sofia 1592

Tel. +359 2 915 3523 Fax

+359 2 915 3525 email:

kzld@cpdp.bg

Website: <http://www.cdpd.bg/>

The exercise of the rights under Regulation EU 2016/679 can be realised by sending a request/application to ProCredit Bank (Bulgaria) EAD in a free text; in order for the request/application to be considered, it should contain the following mandatory particulars that will allow the Bank to identify you:

- Full name;
- Personal Identification Number (PIN)/Personal Number of a Foreigner (PNF)/Date and place of birth (if you are not a Bulgarian citizen);
- Identity document number, date of issuance and issuing authority, validity term;
- Permanent address;
- E-mail address, if you want to receive a response via e-mail;
- In what capacity do you want to exercise your rights under Regulation EU 2016/679 – e.g. client/former client, borrower, mortgage debtor, co-debtor, guarantor, pledgor, employee/former employee, legal representative/proxy/beneficial owner of a commercial company, and, respectively, the name of the commercial company, BULSTAT/Unified Identification Code (UIC)/foreign registration number, or other capacity;
- Description of the request/application to the controller;
- Preferred way of receiving a response from the controller: at the e-mail address/ mailing address specified by you or at a Bank's office specified by you.

It should be noted that if the completed particulars are incomplete and/or inaccurate, we might not be able to identify you and/or to satisfy a part or the whole of your request, respectively.