

## PRIVACY POLICY

ProCredit Bank SH.A. is the data controller of the personal data provided by natural persons when they are using the services that we offer, either through our business outlets or through our online presence when using our website, digital onboarding application, web application, or mobile application.

Hereinafter, the terms “the Bank” and “we” and its derivatives refer to ProCredit Bank SH.A. The term “you” and its derivatives refer to the user of our services. The term “privacy notice” refers to this document. The term “website” refers to <https://www.procreditbank.com.al/> , the “web app” refers to <https://ebanking.procreditbank.com.al/User/LogOn>, and the “app” refers to ProCredit Albania in App Store and ProCredit Mobile Banking Albania in Google Play.

This privacy notice informs you about the collection, use and processing of personal data. The rules outlined in this document apply to any form of data, be them stored electronically, on paper, or on any other storage device.

Controller for the purposes of the Law no. 124/2024 on “On the Protection of Personal Data” and sub legal acts in accordance with this law, is ProCredit bank Sh.a.

Procredit bank has appointed a Data Protection Officer who is accessible for the issue of personal data in the bank as the contacts below:

Mr. Emiljan Dyrmishi

Contact no. +355 (4) 2 389 389

E-Mail: [Emiljan.Dyrmishi@procredit-group.com](mailto:Emiljan.Dyrmishi@procredit-group.com); [HOCCompliance@procredit-group.com](mailto:HOCCompliance@procredit-group.com)

ProCredit Bank Sh.a, Albania

Dritan Hoxha Street, near sport hall” Asllan Rusi”, 1026, Tirana, Albania

[www.procreditbank.com.al](http://www.procreditbank.com.al)

[kujdesindajklientit@procredit-group.com](mailto:kujdesindajklientit@procredit-group.com) ; [informacion@procredit-group.com](mailto:informacion@procredit-group.com)



## Contents

|                                                                                                                   |           |
|-------------------------------------------------------------------------------------------------------------------|-----------|
| <b>1. Data protection principles .....</b>                                                                        | <b>3</b>  |
| <b>2. Definitions .....</b>                                                                                       | <b>3</b>  |
| <b>3. What personal data does the Bank process? .....</b>                                                         | <b>4</b>  |
| <b>4. How does the Bank collect your personal data? .....</b>                                                     | <b>4</b>  |
| <b>5. What are the purposes of data processing? .....</b>                                                         | <b>5</b>  |
| <b>5.1 Decision-making and automated profiling .....</b>                                                          | <b>6</b>  |
| <b>6. What is the legal basis for processing personal data? .....</b>                                             | <b>6</b>  |
| <b>7. How does the Bank process your personal data? .....</b>                                                     | <b>7</b>  |
| <b>7.1 Digital Onboarding .....</b>                                                                               | <b>7</b>  |
| <b>7.2 Loan Origination .....</b>                                                                                 | <b>8</b>  |
| <b>7.3 Transfer by phone .....</b>                                                                                | <b>9</b>  |
| <b>7.4 Biometric authentication .....</b>                                                                         | <b>9</b>  |
| <b>7.5 Human Resources .....</b>                                                                                  | <b>9</b>  |
| <b>7.6 Phone call recordings .....</b>                                                                            | <b>9</b>  |
| <b>7.7 Anonymized datasets .....</b>                                                                              | <b>10</b> |
| <b>7.8 Green financing opportunities .....</b>                                                                    | <b>10</b> |
| <b>7.9 Client referral .....</b>                                                                                  | <b>10</b> |
| <b>7.10 Contactless Payments .....</b>                                                                            | <b>10</b> |
| <b>8. What are your data protection rights? .....</b>                                                             | <b>10</b> |
| <b>9. What are data subject access requests? .....</b>                                                            | <b>11</b> |
| <b>10. When can the Bank transfer your personal data? .....</b>                                                   | <b>12</b> |
| <b>11. What is the period for storing personal data or the criteria for determining the storage period? .....</b> | <b>13</b> |
| <b>12. What are cookies? .....</b>                                                                                | <b>13</b> |
| <b>12.1 What type of general data and information does the Bank collect? .....</b>                                | <b>14</b> |
| <b>12.2 Why does the Bank use cookies and collect general data and information? .....</b>                         | <b>14</b> |
| <b>12.3 How can users manage cookies? .....</b>                                                                   | <b>15</b> |
| <b>13. Google Analytics .....</b>                                                                                 | <b>15</b> |
| <b>14. Data processing in information communication .....</b>                                                     | <b>15</b> |
| <b>15. Privacy Policy Updates .....</b>                                                                           | <b>16</b> |

## 1. Data protection principles

The Bank processes your personal data in accordance with the provisions of Law No. 124, dated 19.12.2024 "On the Protection of Personal Data", (hereinafter referred to as: the Law) and other applicable legal and sub-legal acts in the country. This ensures that the processing of personal data when requesting services from the Bank is in accordance with the safeguards and legally applicable obligations.

The Bank is committed to processing all personal data under its control in accordance with the principles governing their processing. Therefore, personal data:

- Processed lawfully, fairly and transparently
- Collected only for specific, explicit and legitimate purposes
- They are adequate, relevant and not excessive in relation to the purposes for which the data are processed.
- Are accurate and, where applicable, up to date
- They are stored for as long as it is necessary, according to the conditions and deadlines set out in the legislation in force.
- They are processed under appropriate security measures, respecting their integrity and confidentiality.

The Bank is committed to the protection of personal data within its premises and systems. The Bank guarantees that the Bank's employees and companies that provide services to the Bank are obliged to maintain confidentiality in accordance with the provisions of the Law "On the Protection of Personal Data" and with the principles of data protection. The Bank declares that the customer's data will not be used for purposes other than the data that are to be used at the time of their collection or purposes related to the provision of banking products and services directly by it or through the postal service company as well as other third parties, contracted by the Bank and that are licensed to perform the relevant services, in accordance with local and European Union legislation. This also includes entities that perform outsource services for the clients of the Bank, such as: remote identification and verification based on the applicable EU and Albanian legislation in force in our country, delivery of cards through the postal service, etc.

The Client gives his consent for the bank to process and transfer his data, including to third parties, for direct marketing purposes and is aware that this consent may be withdrawn at any time by notifying the bank. The Client gives his consent with full and free will for the control, processing, transfer of his personal data by the bank and third parties, for this purpose but not limited to it.

## 2. Definitions

For the purposes of the privacy policy, the definitions found in the law "On the protection of personal data" apply:

**"Personal data"** is any information relating to a data subject.

**"Controller"** is the natural or legal person and any public authority which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the processing of personal data, in accordance with the provisions of the law, the controller is the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**"Consent"** is any freely given, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by any other unambiguous indication of his or her wishes, signifies agreement to the processing of personal data relating to him or her for one or

more specific purposes.

**"Processing"** is any action or set of actions performed on personal data or sets of personal data, whether or not carried out by automated means, such, such as: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval,

consultation, use, dissemination by transmission, distribution or making available in any other means, linking or combining, limiting, deleting or destroying.

**"Processor"** is the natural or legal person and any public authority which processes personal data in behalf of controller

### 3. What personal data does the Bank process?

The Bank processes personal data to provide its services or when required by law. The category of personal data that will be processed depends on the services requested and the products used by the customers. For example, if you want to make an appointment with the Bank regarding banking services, you must provide your first and last name, telephone number, email address etc.<sup>1</sup> However, if you want to open a bank account, you must provide more personal data. The categories of data that are processed by the Bank are:

- Identity and contacts (name, surname, gender, citizenship, education, address, email, identity document, etc.)
- Financial information (Income details, credit history, ownership documents, etc.)
- Information regarding the products and services offered by the Bank (Details of accounts, cards, transactions, history, etc.)
- Technical information and online identification (such as your credential to log in online, Ip adress)
- Legal records, in the context of assessing the client's legal situation, assessing applications for credit products
- Other types of data (Security camera images, voice recordings, investigative data, complaints, etc.)

### 4. How does the Bank collect your personal data?

The Bank collects your personal data mainly when you use the services and products offered directly at the counter or on our online platforms. The Bank collects your personal data when you:

- Register as a customer and/or open a bank account, on a branch / agency of the bank or online
- Apply for any of our products or services, such as term deposits, home loans, investment loans, etc.
- Use banking services such as e-banking, m-banking, etc.
- Use or view the bank's website through your web browser's cookies.
- the Bank's head offices/agencies/branches
- Contact the Bank via email or contact/complaint forms (or via phone calls via the

---

<sup>1</sup> The Bank processes personal data relating to children only in accordance with legal requirements and after obtaining the consent of their parent/ legal guardian.



Contact Center or other communication channels)

- Provide information, in writing or orally, through email, contact center forms, notarial statements, contracts, or other communication channels.
- When applying for a professional internship, participation in the "Onboarding" employment program, to be employed by the bank.
- When you receive other banking products or services from the bank other than those listed above.

The Bank may collect your data within the limits set out in applicable legislation. Data may also be obtained indirectly through other entities of the ProCredit group, or from other public sources such as:

- Public registers (e.g. Credit Register from the Bank of Albania, Public registers administered by the Central Bank of Albania, Registers administered by the Albanian Credit Register, R.B.S, Other public registers, etc.)
- Public authorities and law enforcement agencies
- Recruitment agencies in cases of employee employment (if applicable), etc.

In any case, personal data is collected and processed in full compliance with the provisions of the legal and sub-legal acts in force in the Republic of Albania.

## **5. What are the purposes of data processing?**

The Bank processes your personal data to provide its services and products, such as financial/banking services and related services. The Bank relies on a number of legal bases for processing personal data. Personal data is used to:

- Process data subject applications for services and products offered by the Bank (credit products, accounts and other services).
- Process payments and other transactions made by and/or to data subjects Whether through methods provided directly by the bank or through other legally recognized services, such as open banking.
- Process data regarding the fulfillment of contractual obligations for each banking product and service
- Providing timely services and high-quality products on time
- Fulfill legal and regulatory obligations (such as reporting and responding to requests from the Bank of Albania, Tax Institutions, Enforcement Service, etc.)
- Verify the identity of data subjects physically or remotely through online platforms certified by the relevant authorities, in accordance with applicable legislation.
- Verified credit rating
- Prevent money laundering, terrorist financing and fraud
- Checked and reported liabilities according to legal requirements
- Improved customer service and customer relationship management and market research through research, analysis/surveys, product promotion, the execution of direct marketing by the bank itself or by third parties, in accordance with the applicable legal provisions.
- Accelerated business development, ensure proper management of credit risk, environmental risk, etc. (especially credit risk)
- Protect the legitimate interests of the Bank (e.g. video surveillance, counting funds, resolving customer complaints, etc.)

### **5.1 Decision-making and automated profiling**

The Bank, as a rule, does not use profiling or fully automated decision-making when establishing business relationships with data subjects. However, verification of the client's identity through the use of technology and other electronic means may be carried out in cases where this process is carried out remotely and without the physical presence of the client in the bank, in compliance with the applicable law. The Bank may also use information technology tools for verification automation for individuals, companies and suspicious transactions, or to identify payments subject to international sanctions in relation to the prevention of money laundering and terrorist financing, and fraud. However, these processes are based on the use of automated means and also can require the involvement of responsible staff in making the final decision and to ask re-evaluation of the case by them, if is necessary.

## **6. What is the legal basis for processing personal data?**

The Bank processes your personal data lawfully if at least one of the following criteria is met:

- The data subject has given consent to the processing of his/her personal data for one or more specific purposes. In such a case, the processing of personal data is permitted on the legal basis of consent, which is revocable at any time. Customers may withdraw their consent through the same form as they gave their consent or through our contact channels free of charge. The withdrawal of consent does not affect the lawfulness of the processing based on consent before its withdrawal. The processing of personal data of a minor based on consent in the context of providing direct services to him/her is lawful if the minor is over 16 years of age. When the minor is under 16 years of age, the processing is lawful only when consent is given or authorized by his/her parent or legal guardian and to the extent that it is given or authorized by him/her.
- The processing is necessary for the performance of a contract to which the data subject is a party or to take steps at the data subject's request prior to entering into a contract. In this case, the processing of personal data is necessary to fulfill contractual and pre-contractual obligations required of you to perform financial services, banking transactions or other services and products of the Bank.
- The processing is necessary for the fulfillment of a legal obligation to which the Bank is subject. In this case, the processing of personal data is justified by fulfilling the requirements of the Law on "Banks in the Republic of Albania", as amended, the Law "On the Prevention of Money Laundering and Financing of Terrorism", as amended, tax legislation, legislation on the enforcement service, other legal obligations and regulatory requirements to which the Bank is subject. Such obligations authorize the Bank to process your personal data to verify your identity, among other things, to prevent money laundering and fraud, assess your financial situation, report obligations due to tax laws and assess risk.
- Processing is necessary to protect the vital interests of the data subject or of another person
- The processing is necessary for the performance by the controller of a legal task carried out in the public interest or when the controller is authorized to exercise public functions, duties or powers under applicable law.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular

where the data subject is a minor, override these interests, except where the processing is carried out by public authorities in the performance of their duties. In this case, your personal data are processed on the basis of applicable national legislation in order to protect the legitimate interests of the Bank or the legitimate interests of a third party institution, to ensure the security of IT systems, to prevent fraud through the processing of device data, to prevent criminal acts, to manage and develop services and products, to manage risk within the ProCredit Group, etc.

## **7. How does the Bank process your personal data?**

The Bank processes data lawfully, fairly and transparently, in compliance with the requirements of applicable laws, providing protection against unauthorized or unlawful processing, and against accidental loss or disclosure of personal data, implementing appropriate technical and organizational measures. For matters related to the protection of personal data, the Bank has appointed a Data Protection Officer. The Bank has also appointed a Data Security Officer.

The Bank implements appropriate technical and organizational measures in a manner that achieves the highest possible security, appropriate to the level of risk, in order to protect your personal data, for example by using equipment and data protection, access control and rights, user identity verification, etc. The Bank may, at the request of the Client, at any time delete all of his personal data<sup>2</sup> collected by the Bank, correct or update them in accordance with applicable legislation. The Bank is also at the Client's disposal at any time for any further questions on data protection and on how the Bank processes the Client's data and who processes this data.

The bank collects and processes your data during the account opening process digitally, remotely and without the need to visit the bank. This solution is provided through remote identification and includes processes such as: collection of identification documents, facial recognition, photos for similarity detection and video recording, as well as electronic signing of contracts. The categories of personal data processed include all data processed for the account opening, such as identification information, contact information, document-based data, such as uploading a photo of your ID card or passport.

To provide services through service providers the bank offers digital account opening via its trusted partners: Fintech OS SRL, which is responsible for integration components, and Onfido Limited together with Namirial S.p.A., who are responsible for the SaaS solution and the provision of the electronic signature certificate for customers. The contractual relationship is governed by a service agreement, which also includes provisions related to data processing and confidentiality obligations.

### **7.1 Digital Onboarding**

The Bank collects and processes your data during the account opening process digitally, remotely and without the need to visit the bank. This solution is provided through remote identification and includes processes such as: collection of identification documents, facial recognition, photos for similarity detection and video recording, as well as electronic signing of contracts. The categories of personal data processed include all data processed for the account opening process, such as identification information, contact information, document-based data, such as uploading a photo

---

<sup>2</sup>According to the conditions provided for in Article 12-20 of Law No. 124 Date 19.12.2024 "On Personal Data Protection"

of your ID card or passport. The Bank collects your personal data during this process for compliance with legal and regulatory requirements for verifying the identity of customers, for the prevention of fraud, such as identity theft and/or the use of false documentation, as well as to fulfill contractual obligations and to improve your customer experience.

To provide services through service providers, the bank offers digital account opening through its trusted partners Quipu GmbH, which is responsible for the integration of Core banking with FintechOS platforms, Onfido Limited together with Namirial spa, which are responsible for the SaaS solution and the provision of electronic signature certificates to customers. The contractual relationship is governed by a service agreement and includes terms and conditions related to data processing and confidentiality obligations.

Facial recognition data is processed based on your explicit consent, with the possibility of choice and is available only to the relevant electronic identification service provider (eIDV) and is stored by the bank for as long as necessary, according to applicable legislation. Your technical data includes IP address, device information, as well as other technical identifiers related to your use of our digital platform. Your personal data is stored only for as long as necessary to fulfill the purposes set out in this section, to comply with legal obligations.

Opening an account digitally with the integration of facial recognition technology offers increased security, fraud prevention and compliance with applicable legislation. This is achieved through the use of advanced technology, encryption, access control and regular security assessments that are implemented to protect your personal data from unauthorized access, disclosure, alteration or destruction. All parties involved in providing the solution are certified according to the best international standards.

## **7.2      Loan Origination**

Loan Origination is a digital solution that the Bank makes available to its customers to apply for consumer loans at lower amounts. When you apply for a digital consumer loan through this solution, the Bank processes your personal data to assess your eligibility, to carry out mandatory checks on your creditworthiness, financial situation and AML/KYC, to prepare and sign loan contracts electronically and to comply with legal and regulatory requirements. Before submitting the application, customers must give their explicit consent for the Bank to have access to the Credit Registry data, as well as to process other data/documents submitted during the loan application.

If you are not already a customer of the Bank, you will first be required to complete the account opening process digitally, as described in section 7.1. In this case, the bank account will only be opened after the approval of your loan application. Loan Origination involves decision-making based on predefined eligibility and credit risk criteria. When all the criteria requested by the client are met, the loan application is automatically approved. When one or more criteria requires additional assessment, the application is sent for manual review by the Bank's employees. The application may be automatically rejected only in cases where mandatory eligibility criteria, such as age, citizenship and minimum income level, or specific credit risk criteria, such as the category in the Credit Registry, are not met. In these cases, you always have the right to request human intervention to review the completed application, express your point of view and object to the decision made on the completed application. The right to request information about the application, to express objection and to complain can be exercised by contacting the Bank through its official communication channels or by visiting its branches.

### **7.3 Transfer by phone**

"Phone Transfer" is a type of intra-bank fund transfer available within the framework of using our application. You can send money to contacts from your mobile phone via Phone Transfer without knowing their bank details if the recipient is also a client of the Bank. To perform this service, the Bank processes data from the sender and the recipient and the transfer can be viewed and listed in the account transaction history.

To use this type of transfer, you have the option to access the contacts stored on your mobile device and search for the contact in the corresponding field. When you wish to use the telephone funds transfer service, the bank requests your electronic authorization to receive this service. In this context, the processing of personal data is permitted on the legal basis of the legitimate interests of the data subject in receiving this service.

### **7.4 Biometric authentication**

Biometric authentication is an optional verification method created by the Bank to access the ProCredit Bank mobile application. It is a fingerprint or facial recognition feature that is designed, released and branded by Apple Inc. and Android respectively. The Bank will not store biometric authentication in its application, nor will it collect it.

Therefore, the bank cannot link it to the personal information it holds about its customers. The bank relies on the device to authenticate and confirm/reject the verification. Therefore, the bank does not process biometric data. You can enable/disable this type of authentication at any time via the application.

### **7.5 Human Resources**

For human resources purposes, ProCredit bank processes the personal data of job applicants, internship applicants, current and former employees.

During human resources management activities, the data collected is processed on the basis of specific laws regulating employment relationships for tax, accounting, occupational health and safety conditions and social security purposes.

The data processed for human resources management purposes include, but are not limited to:

- Identification data such as full name, date and place of birth, age;
- Contact data such as residential address, telephone number and email address.
- Data on education and professional experience, including education history, training, language skills and professional affiliations.
- Information related to the job position, such as position title, function, organizational structure and location of the workplace.
- Other data, as appropriate, that may be necessary for the full realization of human resources management goals.

### **7.6 Phone call recordings**

When you contact us by phone, at the Contact Center number or at the number you received from the bank to obtain an exchange rate, the conversation will be recorded for security purposes, to guarantee the quality of service and as evidence to enable verification of contractual requirements and to prevent and detect fraud. For the processing of this data, the Bank relies on legitimate interest according to the provisions of the law "On the Protection of Personal Data".

Call recordings will be retained for as long as necessary for security and evidentiary reasons, in accordance with the deadlines set out in data protection legislation. If requested, records will

be shared with competent authorities, in accordance with applicable laws. If you do not want your conversation to be recorded when you call us, please contact the bank via email.

### **7.7 Anonymized datasets**

We process your personal data for the purpose of creating anonymized statistics on how clients interact with our products and services, in order to improve product development, analyze customer behavior, and assess the Bank's performance.

These statistics are fully anonymized and do not allow the direct or indirect identification of any individual. Processing is carried out in accordance with the provisions of the Law "On Personal Data Protection."

### **7.8 Green financing opportunities**

The Bank participates in the Programs of International Financial Institutions such as: EIF, EIB, EBRD, CEB, etc. to provide loans to eligible borrowers for various projects such as: youth employment, small and medium-sized enterprises, green investments, etc. These institutions may control and process personal data for the purpose of providing services under these financing schemes.

Therefore, the Bank transfers your personal data, after obtaining your consent, to the relevant institution, partner institutions and/or other partnership support, as well as their Data Processors. The institution acts as an independent data controller and processes your personal data in accordance with the Law "On the Protection of Personal Data".

### **7.9 Client referral**

The Customer Referral feature, when permitted by the Bank, enables existing customers of the bank to invite friends to open an account by sharing their unique referral code. During the digital account opening process, new customers can enter this referral code in an optional field called "Friend Referral Code". If both the referring and referred customers meet the Bank's eligibility requirements, such as successful account activation, disbursing of loan products, etc, each will receive a bonus according to the terms and conditions set by the Bank. No sensitive personal data regarding the referred customer is disclosed to the referring customer.

### **7.10 Contactless Payments**

Customers can use their bank cards for contactless transactions at ATMs and POS, including for payments through platforms such as Apple Pay and Google Pay.

To carry out these transactions, the Bank cooperates with the international card schemes Visa and Mastercard. When a card is registered and used in Apple Pay or Google Pay, the card data is tokenized by Visa or Mastercard, so that the real card number is not used during the transaction.

When using Apple Pay or Google Pay, only the necessary technical information for the payment is processed, while sensitive card data remains protected through tokenization mechanisms. This processing is necessary for the fulfillment of the contractual relationship between the Bank and the Customer.

## **8. What are your data protection rights?**

As a data subject, you have the following rights:

- The right to be informed — You have the right to be informed about the collection and use of your personal data, the purpose of its processing, etc.
- Right of access — You have the right to access and receive a copy of your personal

data.

- Right to rectification and erasure — You have the right to have correct personal data if it is inaccurate or completed if it is incomplete, as well as to have your personal data erased, under certain conditions <sup>3</sup>.
- The right to be forgotten — You have the right to have your personal data erased, under certain conditions, according to the limitations set out in applicable law.
- Right to restriction of processing — You have the right to request restriction of processing of your data when the processing is unlawful, when the processed data is inaccurate, when the controller no longer needs the data.
- Right to data portability — You have the right to receive your personal data held by the Bank and reuse it for your own purposes, such as storing it for personal use or transferring it to another data controller, as defined in applicable legislation.
- Right to object — You have the right to object to the processing of your personal data by the Bank, under certain conditions. For example, you have the right to object to the use of your personal data for direct marketing.
- Rights related to automated decision-making and profiling — You have the right to request from the Bank not to be subject to a decision based solely on automated processing, including profiling, for example, the rejection of an online loan application.

The bank will respond to you without delay and within 30 days of your request if you decide to exercise any of the aforementioned rights. However, taking into account the complexity and the number of requests within a month, this time period may be extended by an additional 30 days. In any case, you will be informed within 30 days from the receipt of the request, along with the reasons for the delay.

In cases where your request is not processed or the fulfillment is refused, you will be informed of the reasons for the non-processing or refusal, as well as of your right to lodge a complaint with the Commissioner and to file a claim before the court.

## 9. What are data subject access requests?

Subjects of personal data and other data held by the Bank have the right to receive the following information:

- The purpose of processing their data
- The importance and consequences of this processing
- Legal basis for processing
- period of retention of personal data or the criteria used to determine this period
- The category of data, even when not collected from the data subject, and any information about the source of these data.
- Information about the recipient(s) of the data, including recipients in foreign countries or international organizations, and how appropriate protection is ensured
- The existence of rights under the law and the right to appeal to the Commissioner.

This information can be requested directly through a request from the data subject made to the person responsible for Data Protection at the bank or via email [alb.dpo@procredit-group.com](mailto:alb.dpo@procredit-group.com). The Bank will always verify the identity of any data subject requesting access before providing any information. The data subject has the right to request whether or not their data is being processed and to receive a response, no later than 30 days from their request.

---

<sup>3</sup> According to the cases defined by the law in Article 15, point 2 thereof.

## **10. When can the Bank transfer your personal data?**

The Bank may transfer personal data to clients, third parties, where such transfer includes the transfer of personal data to the Bank's agencies, to the ProCredit group, members of the ProCredit group, their external auditors, the External Auditors of ProCredit Bank or to other third parties that lawfully process your data. The Client is aware that certain personal data must be transferred to the Bank's parent company headquartered in the Federal Republic of Germany for consolidated reporting and risk management purposes, or to other third parties for the purposes of credit risk assessment, environmental risk assessment, market studies, research, surveys/analysis, promotion of products and services, bank events, etc. If there is a legal or regulatory obligation from public authorities and other institutions (such as the Bank of Albania, the Tax Directorate, Local and Central Tax Institutions, the Customs Directorate, the Financial Intelligence Agency, the Deposit Insurance Agency, Financial Supervisory Authority, Competition Authority, the Private and Public Bailiff Service, the Court, the Prosecutor's Office, Police Bodies, etc.), the Bank allows the use, administration of customer data by these institutions. These institutions also include the Bank's External Auditors or other entities that are part of the ProCredit financial group based in Germany. These institutions are allowed to use the data to the extent necessary and in any case in accordance with the requirements of specific laws.

The bank may transmit your data to:

- **Authorities:** Supervisory authorities and regulatory authorities such as local government, the Central Bank of the Republic of Albania (BOA), AIF, General Directorate of Taxes, IRS, or other law enforcement and Anti-Money Laundering and Counter-Terrorism Financing institutions.
- **Your Authorized Representative:** Individuals or organizations that give instructions or manage accounts, products, or services on your behalf, such as lawyers, brokers, joint account holders, solidary debtors, etc.
- **Third Parties:** Entities with which the Bank must interact to enable payments such as: Mastercard as an issuer of debit/credit cards, commercial banks, correspondent banks, ATM administrators, companies that process card payments, your beneficiaries, SWIFT, SEPA, AIPS, AECH, etc. or institutions such as: AAPSK, AIF, HIDAA, KPK and KPA, BKH, Prosecutors' Offices, Courts, etc.
- **Other financial institutions:** Members of the ProCredit Group. Credit and financial institutions that offer guarantee/credit funds to bank customers, such as the European Investment Fund, European Investment Bank, EBRD, ADGF, CEB, etc.
- **To entities licensed in Albania or in EU countries** to perform remote verification and identification services for bank customers (digital onboarding or Loan Origination), in accordance with applicable banking legislation, legislation on trusted electronic services, etc.
- **Others:** Companies that provide services for the purposes of fulfilling legitimate interests or contractual obligations, such as external legal advisors, notaries, property valuation companies, insurance companies, auditors, accountants, archiving and destruction companies, cloud data storage companies, IT and telecommunications service providers, software development contractors, postal companies, etc.

When the data is transferred, the transfer is made in full compliance with the provisions of Law

No. 124, dated 19.12.2024 “On the Protection of Personal Data”, and when the country or international organization in question ensures an adequate level of data protection.

## **11. What is the period for storing personal data or the criteria for determining the storage period?**

The retention period of personal data depends on the category of data and the purposes for which they are processed. In any case, personal data are processed to the extent necessary for the Bank to fulfill its obligations for the purpose for which the personal data were collected, or as required by applicable legal and regulatory frameworks.

The Bank will process your personal data after the termination of the contractual relationship for a period deemed necessary according to legal and documentation requirements. For example, personal data related to account information are kept for five years from the date of termination of the business relationship with the client. However, the deadlines set out in the applicable legislation on the protection of personal data and other laws apply to the storage of personal data (e.g. the law on the prevention and laundering of money and the financing of terrorism).

The Bank justifies the retention period based on the purposes for processing personal data and complies with legal obligations for data retention. If personal data is no longer required, it will be deleted in accordance with our deletion/destruction processes or anonymized.

## **12. What are cookies?**

The Bank webpage uses cookies. Cookies are text files that are stored on the computer system by the Internet browser. Many websites and servers on the Internet use cookies. Many cookies contain a so-called cookie “ID”. The cookie ID is a unique identifier. It contains a string of characters by which websites and Internet servers can be assigned to the specific Internet browser where the cookie is stored. This allows visited websites and Internet servers to distinguish the individual browser of the data subject from other Internet browsers that contain other cookies. A specific Internet browser can be recognized and identified using the unique cookie ID.

“Cookies” are text files that are sent to your computer so that we can recognize you when you visit us again. They serve to make our service easier to use, more efficient and more secure. You can set your web browser to notify you when you receive a cookie, or to refuse their use.

The websites use the Google Analytics 4 technology (<https://www.google.com/analytics/>) in order to collect visitor data for marketing purposes. The data collected via google analytics 4 will not be used to determine the personal identity of the visitor and will not be combined with other personal data relating to the user, unless the user has previously consented to this. Users may object to the collection and storage of their data at any time.

### **Necessary cookies**

These cookies are necessary for the website to function properly and cannot be disabled in our system. Typically, these cookies are activated by actions in your requests for our services. Examples of these actions are registering, filling in forms or setting your privacy preferences. It is possible to set your browser to block these cookies, but some parts of our website may not function properly when they are blocked.

### **Performance cookies**

We use these cookies to provide statistical information about our website. They are used to improve performance measurement. This category is also known as Analytics. Activities such as counting page visits, page loading speed, bounce rate and the technologies used to access our website are included in this category. We use Facebook pixels for advertising purposes.

**Functional cookies**

We use these cookies to enhance functionality and enable personalization, such as real-time chat, video, and social media usage. These cookies may be set by us or by third-party service providers whose digital services we have added. If you do not allow these cookies, some of these features may not work properly.

**Advertisement**

These cookies are set through our site by our advertising partners. These cookies may be used by third-party companies to create a basic profile of your interests and show you relevant ads on their sites. They identify your browser and device. If you choose not to allow these cookies, you will not be followed by our targeted advertising on other websites.

**12.1 What type of general data and information does the Bank collect?**

The Bank collects a range of general data and information when a data subject is using webpage or an automated system. This general data and information are stored in server logs and contains:

- Browser types and versions used
- The operating system used by the access system
- Websites from which the access system has reached our website (so-called “referrers”)
- Under websites
- Date and time of access to the website
- Internet Protocol address (IP address)
- other similar data and information that could be used in the event of attacks on our information technology systems
- Data processing in information communication

**12.2 Why does the Bank use cookies and collect general data and information?**

The Bank uses cookies to provide website users with quality services that would not be possible without cookies. Cookies enable the information and offers on the website to be optimized with the user in mind. Cookies also allow us to recognize website users. The purpose of this recognition is to make it easier for users to use the website. For example, website users who allow cookies do not need to register access data each time they visit the website, because this function is taken over by the website and the cookie stored on the user's computer system.

When using the above-mentioned general data and information, the Bank does not draw any conclusions about the data subject. In fact, this information is needed to:

- Manage website content
- Optimize website content, including advertising
- Ensure the sustainability of our information technology systems and website technology
- Provide law enforcement authorities with the information necessary for criminal prosecution in the event of cyberattacks

### **12.3 How can users manage cookies?**

The data subject may prevent the setting of cookies by the website at any time by adjusting the relevant settings of the Internet browser used and may thus permanently deny the setting of cookies. Furthermore, cookies that have already been set can be deleted at any time via the Internet browser or other software programs. This is possible in all popular Internet browsers. However, if the data subject deactivates the setting of cookies in the respective Internet browser, not all functions of the website may be fully usable.

### **13. Google Analytics**

ProCredit Bank has integrated the Google Analytics component (with anonymization function) on its website. Google Analytics is a web analytics service. Web analytics is the collection, aggregation and analysis of data regarding the behavior of visitors to websites. The web analytics service collects, among other things, data about the website from which a person came (the so-called referrer), which subpages are visited, or how often and for how long a subpage is viewed. Web analytics is primarily used to optimize a website and to perform cost-benefit analysis of online advertising. The operator of the Google Analytics 4 component is Google LLC. With address, 1600 Amphitheatre Pkwy, Mountain View, CA 94043-1351, United States.

For web analytics through Google Analytics, ProCredit Bank uses the application “gat. Anonymize Ip”. Through this application, the IP address of the data subject in the Internet connection is shortened by Google and anonymized when the data subject accesses our website. The purpose of the Google Analytics component is to analyze traffic on our website. Google uses the data and information collected and, among other things, evaluates the use of our website and compiles online reports showing the activities on our website and provides other services related to the use of our website for us.

Further information and the applicable data protection provisions of Google can be obtained from <https://www.google.com/intl/en/policies/privacy/> and the Google Analytics Terms of Service Google Analytics. Google Analytics is explained further at the following link <https://www.google.com/analytics/>

### **14. Data processing in information communication**

The Bank uses email notifications, SMS notifications and push notifications to inform you about transactions, withdrawals and other information relevant to you. For some of these information communications, we monitor and analyze your user behavior with recent transactions or withdrawals only if this information is relevant for the purpose of the contract or within the scope of our legitimate interests. In certain cases, the Bank may also contact you by phone or via e-banking and m-banking inbox. If you feel that your privacy has been violated, you can appear at any time at one of our agencies at the addresses and hours provided on the website, <https://www.procreditbank.com.al/shq/na-gjeni/>, you can contact us via the phone number +355(4)2389389 and the email address [informacion@procredit-group.com](mailto:informacion@procredit-group.com) and [alb.dpo@procredit-group.com](mailto:alb.dpo@procredit-group.com). Our staff will be ready to provide you with the requested assistance. If users of the Procredit bank Sh.a website are redirected to third-party websites through links placed on it, the Bank is not responsible for the management and personal data protection policies applied by other parties. This privacy policy does not cover third-party websites.



## **15. Privacy Policy Updates**

The Bank reserves the right to modify the privacy notice from time to time in order to reflect new services, changes in our practices and any legal and regulatory changes that may affect our responsibilities to our customers.

*The last change to the Privacy Policy is dated 15.07.2026*