ProCredit Bank
Kosovo

ProCredit Bank Kosovo
Privacy Notice

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, 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-kos.com/, the “web app” refers to https://ebanking.procreditbank-kos.com/, and the “app” refers to ProCredit Kosovo in App Store and ProCredit Mobile Banking Kosovo 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.

For the technical provision of the services, the Bank is supported by Quipu, Steubenhouse Königsberger Straße 1, 60487 Frankfurt am Main. With regard to the processing of data within the framework of our services, there is a written agreement between ProCredit Bank as a client and Quipu as a contractor which governs contract data processing pursuant to Article 27 of the Law no. 06/L-082 on Protection of Personal Data.

Controller for the purposes of the Law no. 06/L-082 on Protection of Personal Data and other provisions related to data protection is:

ProCredit Bank, Kosovo
George Bush Str. no.26
10000 Pristina, Republic of Kosovo

Phone: +383 (38) 555 555 or +383 (0) 49 555 555
Fax: +383 (38) 248 777
kos.info@procredit-group.com
kos.kujdesiperkliente@procredit-group.com
kos.customerservice@procredit-group.com

Data Protection Officer
The Bank has appointed a Data Protection Officer, who is accessible via kos.dpo@procredit-group.com or via our postal address.

Contents:

1. Data protection principles

The Bank processes your personal data in accordance with the provisions of the Law no. 06/L–082 on Protection of Personal Data (hereinafter: the Law) and other, applicable national legislations. This ensures that the processing of personal data when requesting services from the Bank is compliant with the legally enforceable safeguards and obligations.

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

- Processed in a lawful, impartial, and transparent manner (principle of lawfulness, justice, and transparency)
- Collected only for specific, explicit, and legitimate purposes (principle of lawfulness, justice, and transparency)
- Adequate, relevant, and limited to the purposes for which the personal data are processed collected or processed (principle of lawfulness, justice, and transparency)
- Accurate, and where applicable, kept up to date (principle of accuracy)
- Kept no longer than necessary for the purposes for which the personal data are collected or processed, or as required by law (principle of lawfulness, justice, and transparency)
- Processed under appropriate security measures for the personal data (principle of lawfulness, justice, and transparency)

2. Definitions

For the purpose of the privacy notice, the definitions of Article 3 of the Law apply.

- Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- Data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- Data processor means a natural or legal person, from public or private sector which processes personal data for and on behalf of the controller.
- Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
- Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. Which personal data does the Bank process?

The Bank processes personal data in order to provide its services or when it is legally required to do so. The category of personal data to be processed depends on the requested services and products the client uses. For instance, if you want to arrange a meeting with the Bank related to banking services, you have to provide your name and surname, phone number, e-mail address, personal identification number, and region. Nevertheless, for the purposes of opening a current an account, you have to provide more personal data. As such, the personal data that the Bank processes fall into various categories, as provided in the list below. This list, however, is not exhaustive, as the client may be using other services and products which require processing of additional personal data.

Category	Description
Identity and contact information	• Name and surname • Gender • Nationality • Residence status • Identification document or passport (personal identification number, document type, document number, issuing authority, issue date, expiration date) • Birth date • Birth place • Postal address (country, country region, postal code, city, street address) • Contact information (personal e-mail address, home and mobile telephone numbers, work phone number; work e-mail address) • Marital status • Family details • Professional experience • Position and workplace • Education • Authentication data (specimen signature) • Photograph • FATCA status and TIN number • PEP status
Financial information	• Financial status and income details • Employment status and employment of the related persons • Credit history • Credit assessment records • Data from public registers • Relationship with other banks or financial companies • Business records of self-employed individuals • Property documentation (property description, property evaluation report, collateral insurance, construction documentation)
Information related to products and services offered by the Bank	• Data from the fulfilment of the contractual obligations • Bank account details • Credit/debit card details • Transaction details and history • Data related to power of attorney arrangements • Information on any third-party beneficiaries • Other data about the use of products and services offered by the Bank

Category	Description
Technical information and online identification	• 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 the banking services are accessed • Details on the devices and technology you use • Data for merchants that you pay with your card • Data about cookies used by the website
Sensitive categories of personal data	• Health information • Criminal conviction information ** The Bank collects personal data related to children only in compliance with the legal requirements and after having obtained the explicit consent of 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 recordings • Complaints and information in relation to the execution of data subject rights • Investigative data (e.g. sanctions and anti-money laundering checks)

4. How does the Bank collect your personal data?

The Bank collects your personal data mainly when you use the services and products that we offer directly or when you use our online platforms. We collect your personal data when you:

• Open an account and/or are registered as a client
• Apply for any of our products or services, such as term deposits, housing loans, investment loans, etc.
• Use banking services such as e-banking and m-banking, etc.
• Use or view our website via your browser's cookies
• Visit our branches or offices or use the Bank's 24/7 self-service zones
• Contact the Bank via e-mail or a contact form (or through telephone calls via the Call Centre or other communication channels)
• Provide information, either verbally or in writing, via e-mail, contact centre application forms, contracts, or other communication channels

The Bank may collect your data, within the limits permitted by law, also indirectly from legal entities, individuals, other ProCredit group entities, or any other source, including:

• Public registers (e.g. the central credit register, property register, police website for validity verification of ID cards)
• Socially or economically related parties (e.g. employers, business owners, relatives or other persons)
• Public authorities and law enforcement agencies
• Recruitment agencies

5. What are the purposes of personal data processing?

The Bank processes your personal data primarily to produce, offer, and deliver its services and products, such as financial services, and relies on a number of legal bases for personal data processing. Purposes of personal data processing include, but are not limited to.

- Process data subjects' applications for the services and products that the Bank offers
- Process payments and other transactions made to or by the data subjects
- Process data in relation to the fulfilment of contractual obligations for any of the banking products and services
- Provide high-quality and timely services and products
- Meet legal and regulatory obligations (i.e. reporting and responding to the inquiries of the Central Bank of the Republic of Kosovo (CBK))
- Verify the data subjects' identity
- Verify credit ratings
- Prevent money laundering, terrorism financing and fraud
- Control and report obligations as per legal requirements
- Improve customer service and customer relationship management
- Foster business development
- Ensure proper risk management
- Safeguard legitimate interests of the Bank (i.e. video surveillance, clarify cash differences, settle clients' claims, etc.)

Automated decision-making and profiling

The Bank does not use profiling or automated decision-making when establishing business relations with data subjects.

The Bank may, however, use automated decision-making and profiling to screen individuals, companies, and suspicious transactions, or to identify payments subject to international sanctions related to the prevention of money laundering, fraud, and terrorist financing.

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

The Bank processes your personal data if at least one of the following applies:

• The data subject has given consent to the processing of his or her personal data for one or more specific purposes. In such case, processing of personal data is permitted on the legal basis of your consent which is revocable at any time. You can withdraw your consent via the same form as you provided the consent or through our contact channels free of charge. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

• Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. In such case, processing of personal data is necessary to fulfil contractual and pre-contractual obligations requested by you to conduct financial services, banking transactions, or other services and products of the Bank.

• Processing is necessary for compliance with a legal obligation to which the Bank is subject. In such case, processing of personal data is justified according to the Anti Money Laundering Law, tax laws and other legal obligations and regulatory requirements the Bank is subject to. Such obligations authorize the Bank to process your personal data to verify your identity, prevent money laundering and fraud, verify your credit rating, report obligations due to tax laws and risk assessment, among others.

• Processing is necessary to protect the vital interests of the data subject or of another natural person.

• Processing is necessary for the performance of a task carried out in the public interest or in the Exercise of official authority vested in the Bank.

• Processing is necessary for the purposes of the legitimate interests pursued by the Bank or by a third party, except where such interests are overridden by 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 child. In such case, your personal data is processed beyond contractual obligations in order to protect Bank's legitimate interests or the legitimate interests of a third party such as to ensure IT security, to prevent fraud through processing of device data, to prevent criminal acts, for business management and development of services and products, risk management within the ProCredit Group.

• Processing on behalf of the Bank as defined in Article 27 of the Law. In such case, the Bank concludes a contract with the processor with respect to the processing. This contract ensures compliance with the requirements of the Law and defines the sufficient guarantees for the implementation of appropriate technical and organizational measures to ensure protection of your rights.

7. How does the Bank process your personal data?

The Bank processes personal data lawfully, fairly, and in a transparent manner so as to fulfil the requirements of applicable laws by protecting against unauthorised or unlawful processing, and accidental loss or disclosure of personal data using appropriate technical and organisational measures. The Bank has established entities for information security and data protection such as the positions of Data Protection Officer and Information Security Officer.
The Bank implements appropriate technical and organisational measures in a manner that ensures the highest possible level of security that is appropriate for the risk level in order to protect your personal data, for example by ensuring the protection of equipment and data, access control and access rights, user identity verification, etc.

7.1. Video identification and electronic signature

ProCredit Bank is legally obligated to check your identity using a valid identification document within the framework of opening an account and to store particular information from the identification document. For this purpose, we offer you a liveness detection photo and video identification process through our service provider InfoCert S.p.A (hereinafter referred to as "InfoCert"). This process consists of three main sub-processes: identity evidence collection, liveness detection photo and video identification, and electronic signature of documents/contracts. The entire process is carried out directly via the user's mobile phone on a native app (iOS and Android). To conduct the liveness detection photo and video identification process, personal data are collected as proof of your eligibility to use our services.

At the start of the video identification process, our staff will ask for your explicit consent in accordance with Art. 5, Paragraph 1.1 of the Law No. 06/L-082 on Protection of Personal Data to capture the photos and record the conversation. In both cases, your identity is verified by means of a liveness detection photo and video identification process via an encrypted transmission path. ProCredit Bank may transmit personal data to external service providers in order to verify your identity. Regarding the liveness detection photo and video identification process as carried out by InfoCert, we refer you to InfoCert's terms and conditions, which are provided to you during the identification process. The processing of personal data is justified on the basis of Art. 5, Paragraph 1.1 and Paragraph 1.2 of the Law No. 06/L-082 on Protection of Personal Data. After you have authorised us to do so, our staff will access the camera of your end device and take a picture of you, along with a video in which you will be requested to move and then show the front and back sides of your personal identification document or the principal page of your passport. You will be asked to identify yourself directly in the course of the live video session. During the video identification process, our staff must verify the authenticity of your personal identity document or passport. The photo as well as the live video will be recorded and retained for as long as required by law for evidentiary purposes.

7.2. Transfer by phone

The "Transfer by phone" is an intra-bank transfer type available to you within the framework of the use of our app. You can send money to the contacts from your mobile phone via Transfer by phone without knowing their bank details if the recipient is also a customer of the Bank. In order to offer this service, the Bank processes data from sender and recipient and the transfer can be viewed in operations history as well as listed in the account transaction history.
To use this transfer type, you have the option to access the contacts stored on your end device and search the contact to be filled in the respective field. The Bank, however, will not store your phone's contact list and you will have to access it each time you want to use the Transfer by phone. In this context, processing of personal data is permitted on the legal basis of legitimate interests.

7.3. Biometric authentication

Biometric authentication is an optional authentication method offered by the Bank to log in to ProCredit Bank Mobile Banking. It is a fingerprint or face recognition feature that is designed, released, and trademarked by Apple Inc. and Android, respectively. The Bank will never store biometric authentication in its mobile banking app nor collect it. Therefore, the Bank cannot link it to the personal information it holds about its clients. The Bank relies on the device to authenticate and confirm/reject verification. Accordingly, the Bank is not processing the biometric data. You can enable/disable this type of authentication at any time.

7.4. Human Resources

For the purposes of human resources management, the Bank processes personal data of job applicants, current and former employees of ProCredit Bank Kosovo. In the course of human resources management activities, the collected data are processed on the ground of specific laws regulating the labour and civil servants' relationship, for tax insurance, accounting, safe and healthy labour conditions, and social insurance purposes.
Detailed information on how the Bank collects and processes personal data during the recruitment process can be found HYPERLINK here.

8. What are your data protection rights?

As a data subject, you are entitled to 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 right of access — You have the right to access and receive a copy of your personal data.
- The right to rectification — You have the right to rectify your inaccurate personal data or complete it if it is incomplete.
- The right to erasure (right to be forgotten) — You have the right to have your personal data erased, under certain conditions[1].
- The right to restrict processing — You have the right to request restriction of processing your personal data, under certain conditions.
- The right to data portability — You have the right to obtain the personal data that the Bank holds on you and to reuse them for your own purposes, such as storing them for personal use or transmitting them to another data controller.
- The right to object — You have the right to object to the processing of your personal data from the Bank, under certain conditions. For instance, you have the absolute right to object to the use of your personal data for direct marketing.
- Rights in relation 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, automatic refusal of an online credit application.

The Bank will respond without delay and within one month to your request should you decide to exercise any of the abovementioned rights.

You have also the right to send your complaint to the Information and Privacy Agency via their Complain form accessible at https://aip.rks-gov.net/en/complaints/

1. To the extent permitted within the applicable legal framework.

9. What are data subject access requests?

Data subjects whose personal and other data are held by the Bank are entitled to:

- Ask what information the Bank holds about them and why
- Ask how to gain access to it
- Be informed on how to keep it up to date
- Be informed on how the Bank meets its data protection obligations

This information can be requested directly through a subject access request (SAR) made via e-mail at kos.dpo@procredit-group.com. The Bank will always verify the identity of anyone making a subject access request before handing over any information.

10. When can the Bank transfer your personal data?

The Bank may disclose personal data to third parties, in connection with and subject to the services that are being provided, where such disclosure includes the transfer of personal data to affiliates or subsidiaries of the Bank, the ProCredit group, or other third parties who lawfully process your data.

The Bank will only transmit your data to third parties when this is required by law or you have consented to the transmission. The Bank may transfer your personal data to:

- **Authorities:** Supervisory and other regulatory and public authorities such as the local government, the Central Bank of the Republic of Kosovo (CBK), Financial Intelligence Unit, Tax Administration of Kosovo, IRS, other law enforcement and fraud prevention agencies, and the anti-corruption authority.
- **Your authorised representatives:** Individuals or organisations that provide instructions or operate accounts, products or services on your behalf, such as powers of attorney, solicitors, intermediaries, joint account holders, co-debtors, guarantors.
- **Third parties:** Entities the Bank needs to interact with in order to facilitate payments such as Visa, Mastercard, credit card issuers and merchant banks, correspondent banks, ATM administrators, card payment processing companies, your beneficiaries, SWIFT,TARGET 2 SEPA, national clearing or settlement systems, so-called KIPS, RLB (bank account registry), the Pledge Registry managed by MTI and Mortgage Registry managed by the Cadastral Office.
- **Other credit or financial institutions:** Members of the ProCredit group, or credit and financial institutions providing funding, such as the European Investment Fund.
- **Others:** Companies that provide services for the purpose of fulfilling our legitimate interests or contractual obligations, such as external legal advisers; 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 and printing companies.

When data are transferred, the transfer takes place in strict accordance with the provisions of Law no. 06/L – 082 on Protection of Personal Data and only if the country or the international organisation in question ensures an adequate level of data protection.

11. What is the personal data retention period or the criteria for determining the retention period?

The retention period of personal data depends on the category of the data and the purposes for which they are processed. In either case, personal data are processed as long as necessary for the Bank to perform its obligations in light of the purpose for which the personal data were obtained, or as required by the applicable legal and regulatory frameworks.

The Bank will process your personal data after the end of the customer and contractual relationship for a period deemed necessary at any given time according to the legal and documentation requirements.

For example, personal data related to account information are retained for six years from the date of account closure.

The Bank justifies the retention period based on the purposes for processing personal data and it complies with the statutory obligations for retaining data. If personal data are no longer required, they will be erased in accordance with our erasure processes or anonymised, i.e. stripped of all possible identifying characteristics.

12. What are cookies?

The Bank's website uses cookies. Cookies are text files that are stored in a computer system via an Internet browser. Many Internet sites and servers use cookies. Many cookies contain a so-called cookie "ID". A cookie ID is a unique identifier. It consists of a character string through which Internet pages and servers can be assigned to the specific Internet browser in which the cookie was stored. This allows visited Internet sites and servers to differentiate the individual browser of the data subject from other Internet browsers that contain other cookies. A specific Internet browser can be recognised and identified using the unique cookie ID.

Necessary cookies
These cookies are necessary for the website to function properly and can't be switched off in our system. Usually these cookies are set by your actions in your requests for our services. Examples of these actions are logging in, filling in forms or setting your privacy preferences. It is possible to make your browser block these cookies, but some parts of our website may not work properly when these are blocked.

Performance cookies
We use these cookies to provide statistical information about our website. They are used for performance measurement and improvement. This category is also known as Analytics. Activities like page visits counting, page loading speed, bounce rate and technologies used to access our site are included in this category.

Functional cookies
We use these cookies to enhance functionality and allow for personalization, such as live chats, videos and the use of social media. These cookies can be set by ourselves or by our third party service providers, whose digital services we have added. If you do not allow these cookies, some of these functionalities may not work properly.

Advertising
These cookies are set through our site by our advertising partners. These cookies can be used by third party companies for creating a basic profile of your interests and show you relevant ads on other websites. They identify your browser and your device. If decide to disallow these cookies, you will not be tracked by our targeted advertising across other websites.

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

The Bank collects a series of general data and information when a data subject or automated system calls up the website. This general data and information are stored in the server log files and include:

- The browser types and versions used
- The operating system used by the accessing system
- The website from which an accessing system reaches our website (so-called “referrers”)
- The sub-websites
- The date and time of access to the Internet site
- The Internet protocol address (IP address)
- Any other similar data and information that may be used in the event of attacks on our information technology systems
- Data processing in informational communication

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

The Bank uses cookies to provide the users of the website with more user-friendly services that would not be possible without the cookie setting. Cookies enable the information and offers on the website to be optimised with the user in mind. Cookies also allow us to recognise website users. The purpose of this recognition is to make it easier for users to utilise the website. For example, website users who allow cookies do not have to enter access data every time they visit the website, because this function is taken over by the website, and the cookie is thus stored on the user’s computer system.

When using the abovementioned general data and information, the Bank does not draw any conclusions about the data subject. Rather, this information is needed to:

- Deliver the content of the website correctly
- Optimise the content of the website, including advertising
- Ensure the long-term viability of our information technology systems and website technology
- Provide law enforcement authorities with the information necessary for criminal prosecution in the event of a cyberattack

12.3 How can users manage cookies?

The data subject may at any time prevent the placement of cookies by the website by adjusting the corresponding setting of the Internet browser used, and may thus permanently deny the placement of cookies. Furthermore, cookies that have already been placed may 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 placement of cookies in the respective Internet browser, not all functions of the website may be entirely usable.

13. Google Analytics

On its website, ProCredit Bank has integrated the component of Google Analytics (with the anonymizer function). Google Analytics is a web analytics service. Web analytics is the collection, gathering, and analysis of data about the behaviour of visitors to websites. A web analysis service collects, inter alia, data about the website from which a person has come (the so-called referrer), which sub-pages were visited, or how often and for what duration a sub-page was viewed. Web analytics are mainly used for the optimization of a website and in order to carry out a cost-benefit analysis of Internet advertising. The operator of the Google Analytics component is Google Inc., 1600 Amphitheatre Pkwy, Mountain View, CA 94043-1351, United States.
For the web analytics through Google Analytics ProCredit Bank uses the application "_gat. _anonymizeIp". By means of this application the IP address of the Internet connection of the data subject is abridged by Google and anonymized when accessing our websites. The purpose of the Google Analytics component is to analyse the traffic on our website. Google uses the collected data and information, inter alia, to evaluate the use of our website and to provide online reports, which show the activities on our websites, and to provide other services concerning the use of our Internet site for us.
Further information and the applicable data protection provisions of Google may be retrieved under https://www.google.com/intl/en/policies/privacy/ and/or http://www.google.com/analytics/terms/us.html. Google Analytics is further explained under the following link https://www.google.com/analytics/.

14. Data processing when using the customer chat function

If you use the customer chat (ProBot) function on our website or through our app, your IP address and the information you provide to us in your chat communication will be collected and processed. We process your data to the extent necessary to fulfil a contract with you or to carry out pre-contractual measures you have requested. In addition, we process your data within the scope of our legitimate interests as far as this is necessary to answer your general questions about our services and products and to help you find information about our new services and products.

15. Data processing in informational communication

The Bank uses informational emails, inbox, and push notifications to inform you about transactions, withdrawals, and any other relevant information to you. For some of such informational communications, we screen and analyse your user behaviour such as recent transactions or withdrawals only if such information is necessary for the performance of the contract or within the scope of our legitimate interests

16. Updates to the privacy notice

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 towards our clients. The “Last updated” legend at the top of the privacy notice indicates when this document was last revised. Any and all changes become effective when posted on our online presence.