DATA PRIVACY POLICY OF PROCREDIT BANK JSC

January 2025

Functional area of organization:	**Risk Management, Compliance and AML Department**
Regulations:	**Data Privacy Policy within CB "ProCredit Bank" JSC**
Responsible:	**Information Security Specialist - responsible for data protection**
Access level:	**Information with public access**
Original language:	**Romanian**
End users of the document:	• **All employees/freelancers** • **Individual clients, potential clients of the Bank**

REVISIONS

Version	Date of approval by the Bank's Supervisory Board	Effective date	Content of the changes
1.0	29.04.22	11.05.22	Implementation
2.0	30.05.23	06.06.23	Modified section 3, adjusted section 4, modified section 9, adjusted section 11, modified section 12, 13.
3.0	28.06.24	05.07.24	Annual revision, no significant modifications
4.0	28.01.25	04.02.25	Modified section 3, section 4

CONTENTS:

1. General provisions

The commercial bank ProCredit Bank JSC was registered on 25.10.2007 in the State Register of Legal Entities with the state identification number – fiscal code (IDNO) – 1007600059183, and operates as a financial institution under licence Series A MMII No. 004497, issued on 29.01.2018 for an indefinite period, by the National Bank of Moldova, headquartered in Chisinau, MD-2005, No. 1 Grigore Vieru Ave., tel. (373 22) 822501.

ProCredit Bank JSC has the status of data controller and data processor of personal data under the terms of Law no. 133 of 08.07.2011 on the protection of personal data provided by natural persons when they are using the services that we offer, either through the Bank's branches and agencies, or when using our website, web application, or mobile application.

In the following, the terms "Bank" and "we", as well as their derivatives, refer to commercial bank ProCredit Bank JSC (headquarters: Bd. Stefan cel Mare si Sfant 65, of. 901, Chisinau, Republic of Moldova). The term "You" and its derivatives refer to the user of our services, platforms and online applications. The term "Data privacy policy" refers to this document. The term "website" refers to https://www.procreditbank.md/, https://www.procreditbank-direct.com/moldova/ro, https://hr.procredit-group.com/md, "web application" refers to https://eba.procreditbank.md, and "application" refers to CB ProCredit Bank JSC in the App Store and ProCredit Mobile Banking Moldova in Google Play.

This data privacy policy describes how we process personal data. The rules outlined in this document apply to any form and type of data, whether stored electronically, in paper form or in any other storage device.

2. Terms and definitions

Personal data subject's consent – any freely given, expressly and unconditionally indication of will, in written or electronic form, according to the requirements of the electronic document, by which the personal data subject signifies their agreement to personal data relating to them being processed.

Profiling – a form of automatic processing of personal data which involves the use of personal data to assess certain aspects relating to a natural person, in particular to analyse or establish aspects of their performance at work, their economic situation, health, preferences, interests, reliability, behaviour, location and travel.

Personal data (PD) – any information relating to an identified or identifiable natural person ("personal data subject"). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

Recipient – a natural or legal person governed by public law, or by private law, including public authorities and their territorial subdivisions to whom personal data are disclosed, whether a third party or not. The bodies responsible for national defence, state security and public order, the prosecution bodies and the courts, which may receive personal data in the framework of exercising their duties established by law, shall not be regarded as recipients.

Depersonalisation of data – this practice refers to the alteration of personal data so that details of personal or material circumstances can no longer be linked to an identified or identifiable natural person, or any such link can only be made within an investigation with disproportionate efforts, expense and use of time.

Controller – a natural or legal person governed by public law, or by private law, including public authorities, agencies or any other body which alone or jointly with others determines the purposes and means of the processing of personal data expressly provided by applicable law.

Processor – a natural or legal person governed by public law, or by private law, including public authorities and their territorial subdivisions, which process personal data on behalf of the controller, on instructions from the controller.

Processing of personal data – any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, keeping, restoring, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Personal data filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Third party – a natural or legal person governed by public law, or by private law, other than the personal data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the personal data.

3. Data protection principles

The Bank is fully compliant with the normative acts that govern the protection and confidentiality of data, especially Law no. 133 of 08.07.2011 regarding the protection of personal data. This ensures that the Bank's measures to protect natural persons with regard to the processing of their personal data when they request services from the Bank are compliant with the legally enforceable safeguards and obligations.

The Bank undertakes to process the personal data in its possession in accordance with the provisions of the legislation in force and the applicable international norms, which regulate the protection of personal data.

The Bank shall be responsible for complying with and ensuring the implementation of the following principles:

legality, fairness and transparency – the Bank will ensure that it processes personal data lawfully, transparently and fairly towards the data subject;

purpose limitation – The Bank will ensure that personal data are collected for specified, explicit and legitimate purposes and are not further processed in a way incompatible with these purposes;

data minimization – The Bank will process personal data that are adequate, relevant and non-excessive regarding the purpose for which they are collected and / or further processed;

accuracy of the data – The Bank must take all necessary measures to ensure that the personal data are accurate and, if necessary, to be updated, and those that are inaccurate or incomplete from the point of view of the purpose for which they are collected and subsequently processed are deleted or rectified;

limitation related to storage – The Bank will ensure the storage in a form that allows the identification of the subjects of the personal data for a period that will not exceed the time necessary to achieve the purposes for which the data are collected and subsequently processed;

integrity and confidentiality – the Bank will process personal data in a way that will ensure the adequate security of the personal data, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, by taking appropriate technical or organizational measures.

Note: If you have any questions or suggestions, need for informational support regarding this Policy, or you wish to exercise your rights as a data subject, you can contact us using the following contact details:

To: Data Protection Officer
E-mail: mda.Datepersonale@procredit-group.com.
Tel: +373-22-782-477

4. Which personal data does the Bank process?

The bank processes personal data until the initiation of the business relationship, as well as during its development, in strict accordance with the provisions of the legislation in force.

Thus, the Bank processes the following categories of personal data within the banking activity it carries out:

a) Last name, first name, father's name (if applicable)

b) Identification number of the natural person (IDNP) or other unique identification element (if applicable)

c) Last name, first name of the effective beneficiary (if applicable)

d) Last name, first name of family members

e) Date and place of birth

f) Citizenship and residence

d) Signature

h) Data from civil status documents

i) Telephone number/fax/e-mail address

j) Home address/domicile/contact: country, region, county, street, block number, apartment number, postal code

k) Job, profession, sector of activity, professional status, name and address of the employer, work telephone number

l) Political exposure (if applicable) and public office held (if applicable)

m) Level of education and professional training – diplomas obtained

n) Family situation (children, spouse, dependents)

o) Economic and financial situation (salary, income, pensions and other receipts)

p) Data on the assets held

q) Bank details

r) Bank card data

s) Type of identity document held

t) Series and number of the identity document

u) Other data related to identity documents

v) Health data, processing is necessary for the protection of public health

w) The IP address from which the client accesses SADD and records transactions/operations

x) Recorded phone calls

y) Images recorded on video cameras

Note: For example, if an individual wants to arrange a meeting/conversation with the Bank regarding banking services, they must provide their first and last names, telephone number, e-mail address, ID card number and series.

5. How does the Bank collect your personal data?

The Bank collects personal data mainly at the initiation of the business relationship, as well as during the development of this relationship, which you provide directly or when you use our online platforms. We collect your personal data when you:

- Open an account and/or register as a customer.
- Apply for any of the Bank's products or services such as current/savings accounts, term deposits, housing loans, investment loans, etc.
- Use banking services such as ProBanking and MobileBanking, etc.
- Use or view the Bank's website via your browser's cookie modules.
- Visit the Bank's Head Office, branches or agencies, or use the 24/7 Self-Service areas of the Bank.
- 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, by registering Contact Centre application forms through the website or other communication channels.
- Sends the CV for use for recruitment purposes or if it informs in any other way (by e-mail) that it is interested in filling positions within the Bank / participating in internships;
- Join the Bank as an employee.

The refusal to provide personal data may determine the impossibility of providing banking services or fulfilling the other processing purposes by B.C. ProCredit Bank S.A.

6. Subjects of personal data

The processing of personal data by the Bank concerns the data of the following categories of persons:

- Clients – natural persons
- Potential clients of the Bank
- Employees of the Bank/freelancers
- Contact persons, legal or conventional representatives, employees or natural persons appointed by a client of the Bank, co-debtors, guarantors, real beneficiaries, as well as their family members
- Natural persons acting on behalf of business clients: administrators or persons authorised to manage the account and/or founders, associates, beneficial owners, including individual entrepreneurs, members/founders of agricultural farms, persons mentioned in the specimen signature sheet
- Candidates for a job with the Bank; students who embark upon an internship at the Bank or have attended training sessions
- Visitors to the Bank's premises, where video surveillance cameras are installed,

without any scope to identify the person
- Visitors to the Bank's official website, including the Bank's official pages on social networks, and automated remote banking applications

7. What are the purposes of personal data processing?

The Bank processes personal data primarily to offer and deliver its services and products, such as financial services (or employment) and relies on a number of legal bases for processing personal data.

Personal data are used 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
- Verify the data subjects' identity
- Implementation of the measures to prevent and combat money laundering and terrorist financing
- Control and report in accordance with legal requirements
- Improve customer service and customer relationship management
- Ensure proper risk management
- Safeguard legitimate interests of the Bank (for example, video surveillance, clarification of cash differences, resolving customer complaints, etc.)
- Employ persons at the Bank/applying to internships/concluding contracts with freelancers.

The Bank does not use profiling/profile creation or automated decision-making when establishing business relationships with data subjects.

In exceptional situations, by way of derogation from those mentioned above, the Bank may use automated decision-making and profiling/profile creation to verify suspicious persons, companies and transactions or to identify payments subject to international sanctions related to the prevention of money laundering, fraud and terrorist financing.

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

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

- The natural person has consented to the processing of personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is a party or for taking measures before the conclusion of the contract, at the request of the natural person
- Processing is necessary for compliance with a legal obligation to which the Bank

is subject
- Processing is necessary to protect the vital interests of the data subject or another natural person
- Processing is necessary for the execution of a task carried out in the public interest or in the exercise of the attribution conferred on the Bank, within the limits and conditions of the national legislation in force
- Processing is necessary for the achievement of a legitimate interest pursued by the Bank or a third party, provided that this interest does not prejudice the interests or fundamental rights and freedoms of the data subject

9. Conditions for consent

If the processing of personal data is necessary, but there is no legal basis for this processing, the Bank obtains consent from the data subject.

At the same time, in the case of the subject of adult or minor personal data who is subject to the judicial protection measure in the form of guardianship, the consent to the processing of personal data is granted, in written form, by the legal representative, in the case of the minor, or by the guardian, in the case of the adult.

Consent can be revoked at any time using the same form in which it was given. Withdrawal of consent cannot have retroactive effect.

10. How does the Bank process your personal data?

The Bank processes personal data in a lawful, fair, and transparent manner, so as to meet and comply with applicable legislative requirements, by protecting against unauthorised or unlawful processing, loss or accidental disclosure of personal data, using corresponding technical and organisational measures. In this regard, the Bank has established entities for information security and data protection such as the Data Protection Officer and the Information Security Specialist.

The Bank implements appropriate technical and organisational measures in a manner that ensures the highest possible level of security appropriate for the risk in order to protect personal data, by ensuring the protection of equipment and data, access control and access rights, user identity verification, etc.

In cases where personal data are processed on behalf of the Bank, the Bank concludes an individual contract with the person authorised by the data controller which clearly stipulates that the person authorised by the data controller is subject to the same obligations regarding personal data protection, so as to ensure that they comply with legal requirements and implement the necessary technical and organisational measures to protect the rights of the data subject.

11. What are your data protection rights?

As a data subject, a natural person has the following rights:

a) **the right to information** – the data subject has the right to be informed about the identity of the controller or of the processor, about the purpose of processing this data and the recipients of the collected personal data

b) **the right to access** – the data subject has the right to exercise the right of access to personal data processed by the Bank, upon request, without delay and free of charge the information provided within art. 13 para.(1) from Law no. 133/2011 2011 on personal data protection

c) **the right to rectification** – the data subject has the right to exercise the right of intervention on the personal data processed by the Bank, including for the purpose of the rectification, update, blocking or erasure of personal data, the processing of which does not comply with this law, in the sense of art. 14 of Law no. 133/2011 on personal data protection

d) **the right to object:**
i) the data subject has the right to object at any time, free of charge, for well-founded and legitimate reasons related to a particular situation, to their personal data being processed, insofar as this does not contradict the conclusion, modification, execution and termination of the contract

ii) the data subject has the right to object at any time, free of charge and without any justification, to the processing of personal data by the Bank for the purpose of direct marketing within the meaning of art. 16 of Law no. 133/2011 on personal data protection

f) **the right to not be subject to an individual decision -** the data subject has the right to request the annulment, in whole or in part, of any individual decision which produces legal effects on his rights and freedoms, being based solely on the automated processing of personal data intended to evaluate certain aspects of his personality, such as professional competence, credibility, conduct and the like.

g) **the right to have access to justice** - any person who has suffered damage as a result of an unlawful processing operation of their personal data, or their rights and interests guaranteed by Law no. 133/2011 on personal data protection have been violated, shall have the right to refer in a court in order to repair the material and moral damages

The Bank will respond without delay and within 15 days to the data subject's request, and if this term is not sufficient, the Bank reserves the right to extend the response by another 15 days, with the prior notification of the data subject, if they decide to exercise any of the rights mentioned above.

12. When can the Bank transfer personal data?

The Bank may disclose personal data to third parties, in connection with and subject to the services that are provided, if this disclosure includes the transfer of personal data to the Subsidiary institutions of ProCredit Holding and ProCredit Holding - or other third parties in accordance with the applicable legal bases, depending on the situation and only under the conditions that ensure full confidentiality and security of the data.

The Bank will transfer personal data to third parties only when this is required by law or if the data subject has given consent to this transmission. The bank can transfer personal data to the following recipients:

- The Bank's authorised persons, other natural/legal persons who process personal data on the Bank's behalf (e.g. attorneys/lawyers, consultants, accountants, auditors)
- Partners of the Bank (e.g. credit bureaus, intermediaries, insurance-reinsurance companies, etc.), inside and outside the country, based on the agreements concluded with them, related to the supply of products and services
- Competent authorities (e.g. judicial authorities, police, National Centre for Personal Data Protection, the National Bank of Moldova, National Anticorruption Centre, central/local public authorities)
- American authorities (US Treasury Department), if the clients intend to make international transfers through SWIFT (Society for Worldwide Interbank Financial Telecommunication), in order to comply with the provisions of national legislation regarding the prevention and combating of money laundering and terrorist financing
- The US State Fiscal Inspectorate (Internal Revenue Service, USA) for clients who fall under FATCA
- Entities with which the Bank must interact to facilitate payments, such as Visa, card issuers and commercial banks, correspondent banks, card payment processing companies, clients' beneficiaries, SWIFT systems, SAPI, national CNAM/CNAS systems
- Cloud storage companies; IT and telecommunications service providers; contractors of software development

We inform you that all the recipients mentioned above process your data exclusively in order to fulfill the purpose for which it was collected.

13. To which countries or international organisations can the Bank transfer personal data?

Currently, in order to fulfil the above-mentioned purposes, CB ProCredit Bank JSC can transfer certain categories of personal data outside the Republic of Moldova, in the EU/EEA states: the Federal Republic of Germany, Romania, the Republic of Ireland, and the Netherlands, and outside the EU/EEA: the United States of America for the purpose of applying FATCA legislation, where necessary.

At the same time, personal data constitute bank secrecy and are provided to third parties only in accordance with the provisions of art. 96 and 97 of the Law on the activity of banks no. 202 of 06.10.2017 *(in force 01.01.2018).*

For transfers outside the EU/EEA, ProCredit Bank will base the transfer of personal data, based on the standard contractual clauses for the cross-border transmission of personal data, developed and approved by the Centre or with the consent of the subject of the personal data, by informing about the possible risks that such transfers may entail for the data subject as a result of the lack of an adequacy decision on the level of protection and adequate safeguards.

By way of exception, if the Clients of B.C. ProCredit Bank S.A. request through the bank transactions to beneficiaries located in third countries that have not been recognized an adequate level of protection of personal data, the transfer of data to those countries is based on the provisions of Law no. 133/2011 according to which: the transfer that is necessary for the performance of a contract between the bank and the Client or for the application of pre-contractual measures adopted at the request of the Client or, as the case may be, the transfer that is necessary for the conclusion of a contract or for the performance of a contract concluded in the interest of the data subject

14. What is the personal data storage period or the criteria for determining the storage period?

The storage period of personal data depends on the category of data and the purposes for which they are processed. In both cases, personal data are processed as long as necessary for the Bank to fulfil its obligations according to the purpose for which the personal data were obtained or according to the requirements of the applicable legal and regulatory framework.

The Bank will process personal data after the conclusion of the collaborative and contractual relationship for a period deemed necessary at a given time, according to legal and normative requirements.

Thus, after the termination of business relations, the Bank will keep the personal data related to the client for a period of:

- 5 years – on paper
- Thereafter up to 5 years in electronic format

In the event of a request from the Prevention and Combating of Money Laundering Service or the National Bank of Moldova, the record-keeping period can be extended for the requested period, but not more than another 5 years.

15. 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.

16. What type of data and general information does the Bank collect when the Bank's online platforms are used?

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

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

The bank uses cookies to provide website users with more user-friendly services that would not be possible without the use of the cookies. Cookies allow the information and offers on the site to be optimised with the user in mind. Cookies also allow us to recognise website users. The purpose of this recognition is to facilitate the use of the site by users.

When using the data and general information mentioned above, 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

Note: For example, website users who allow cookies do not have to enter access data every time they visit the website, as this function is taken over by the website, and the cookie is thus stored on the user's computer system.

18. 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.

19. Google Analytics

On its website, CB ProCredit Bank JSC has integrated the Google Analytics component (with the anonymisation function). Google Analytics is a web analysis 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 optimisation 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 Amphitheater Pkwy, Mountain View, CA 94043-1351, United States.
For web analysis 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 anonymised when the data subject accesses our website. 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 to us.

Additional information and applicable Google data protection provisions can be found at https:// www.google.com/intl/en/policies/privacy/ and at http://www.google.com/analytics/terms/us.html
Google Analytics is further explained at the following link https://www.google.com/analytics/

20. Updates to the data privacy policy

The Bank reserves the right to change the data privacy policy from time to time to reflect new services, changes in our practices, and any legal and regulatory changes that may affect our responsibilities to our customers, partners and the Bank's employees/freelancers.

21. Final provisions

The responsibility for maintaining this policy in its current state rests with the lawyer appointed in charge of the Legal Section – the person responsible for data protection.

In the event of modifications to the legislation of the Republic of Moldova, or the modification or implementation of standards, normative-methodical recommendations, and requirements of competent bodies, this policy is to be applied, insofar as it does not contradict the adopted normative acts. If necessary, the respective unit will initiate the procedure for amending this policy in the order established by the Bank.

Modification of this policy will take place periodically or ad hoc:

- The periodic modification is to be carried out at least annually.
- The ad hoc modification can be carried out based on the results of the analysis of incidents related to information security, the actuality, sufficiency and efficiency of the measures to ensure the information security applied, based on the results of the informational security audit carried out internally and other control activities.