

PO- 202/ 28/11/2024 DATA PROTECTION POLICY

VERSION NUMBER 1.1

Date of adoption:	28/11/2024
Effective from:	28/11/2024
Approved by:	Management Board with consent of Supervisory Board
Owner:	Compliance Department
Applies to:	All employees in the bank and external partners
Confidentiality:	Public

Contents

EXECUTIVE SUMMARY.....	3
I. PRELIMINARY PROVISIONS.....	3
I.1. References.....	3
II. GENERAL PROVISIONS.....	4
II.1. Object.....	4
II.2. Terms and definitions:.....	4
II.3. SCOPE.....	5
III. DETAILED PROVISION.....	5
III.1. HOW AND WHAT TYPES OF PERSONAL DATA BANK COLLECTS.....	5
III.2. PURPOSES OF THE PERSONAL DATA COLLECTION	7
III.3. AUTOMATED PROCESSING.....	7
III.4. RIGHT ON ACCESS TO PERSONAL INFORMATION.....	8
III.5. PROTECTION OF THE PERSONAL DATA.....	8
III.6. DATE SUBJECT'S RIGHTS.....	9
III.6.1. The right to access personal data.....	9
III.6.2. The right to correction of personal data	9
III.6.3. The right to restrict the processing of personal data	9
III.6.4. The right to object	9
III.6.5. The right to erasure ("right to be forgotten").....	9
III.6.6. The right of a person to data portability.....	9
III.6.7. The right to revoke consent.....	10
III.7. EXCERCISE YOUR RIGHTS.....	10
III.8. FILING A COMPLAINT TO THE SUPERVISORY BODY	10
IV. CLOSING PROVISIONS.....	10
V. HISTORY OF THE VERSION	11

EXECUTIVE SUMMARY

Crnogorska komercijalna banka AD Podgorica (hereinafter referred as: "the Bank") is committed to developing, operating and applying such a regulatory, executive and control system which ensures the safekeeping and protection of bank secrets, securities secrets as well as personal data in accordance with the criteria specified in relevant legal acts and its fundamental business interests.

The personal data processed by the CKB Bank include in particular data required for identifying and liaising with customers, data required for the provision of a given service and/or data generated and processed in the course of the provision of the given service (including data related to debt collection), , the data of the communication – performed on any communication channel – between the CKB Bank and the data subject.

The legal framework for the protection of personal data is determined by the Law on personal data protection („Official Gazette MN“, no. 079/08 from 23.12.2008, 070/09 from 21.10.2009, 044/12 from 09.08.2012, 022/17 from 03.04.2017), (hereinafter referred to as "the Law").

The Bank processes personal data in a legal, transparent and fair manner.

I. PRELIMINARY PROVISIONS

I.1. References

- a) Law on Credit Institutions;
- b) Law on Personal Data Protection;
- c) OTP Group Regulation;

II. GENERAL PROVISIONS

II.1. Object

When processing personal data and transferring it to third parties, CKB Bank respects fundamental rights and fully ensures the principles of data protection all the time. Accordingly, it ensures:

- that personal data shall be processed lawfully, fairly and in a transparent manner for data subjects;
 - that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
 - that personal data processed shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - that personal data processed shall be accurate and, where necessary, kept up to date and CKB Bank takes every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified;
 - that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
 - that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;
- CKB Bank as data controller requires 3rd parties (joint controllers, data processors, independent controllers) with whom the data is shared to comply with the principles laid down in the legislation and supervisory requirements.

OTP Bank and CKB Bank as a member of the OTP group concerned process data, facts and information which are personal data, bank, securities and fund secrets, which they receive, ensuring high level of protection.

The CKB Bank can use the data of its clients available for the purpose of analysis, data will be used for tailoring and offering personalized offers if the client consented to it and uses data on legitimate interest for product developing and analysis aimed at making business decision.

II.2. Terms and definitions:

- (1) **Bank:** CKB Bank a.d. Podgorica;
- (2) **Law:** Law on Personal Data Protection
- (3) **Policy:** Data Protection Policy
- (4) **Personal Data:** any information relating to an identified or identifiable natural person;
- (5) **Data Subject:** shall mean a natural person who is identified or can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

- (6) **Consent:** free statement given in writing or orally on record by which an individual signifies his agreement to personal data relating to him being processed for a specific purpose;
- (7) **Supervisory Body:** Agency for Personal Data Protection and Free Access to Information

II.3. SCOPE

Data Protection Policy (hereinafter referred as „Policy“) applies to all personal data of the Bank's Client that the Bank processes or determines the purpose and manner of processing, as well as to other persons listed in this item.

The Policy applies to all services and products of the Bank that include the processing of personal data. If the basis for processing is consent, the last expression of the will of the data subject, by which that person gives consent for the processing of personal data, applies to all services and products of the Bank used by that person.

The Policy is primarily intended and refers to:

- a) Natural persons who submit a request or use the services and products of the Bank (Clients);
- b) Natural persons interested in using the services and products of the Bank (Potential Clients),
- c) Other natural persons whose data the Bank obtains during its operations in accordance with applicable legal regulations.

The Policy does not apply to anonymised data, ie to data on the basis of which the identity of a person is not directly or indirectly identifiable. Anonymised data is data that has been changed in such a way that it cannot be linked to a specific natural person and therefore, in accordance with the applicable regulations, it is not considered personal data.

The Bank processes personal data for different purposes, and the means of collection, the legal basis for processing, use, disclosure, and retention periods may differ depending on the purpose.

III. DETAILED PROVISION

III.1. HOW AND WHAT TYPES OF PERSONAL DATA BANK COLLECTS

The Bank collects personal data in the following ways:

- Directly from the Client or Potential Clients, by direct delivery by the Client and / or Potential Client (such as when submitting a request for service at points of sale, during communication of the Client / Potential Client with the Contact Center or through the website and social networks, when filing an objection and the like).
- Automatically when using the Bank's products and services, if it is necessary for the Client / Potential Client to enter their data in order to use the appropriate product and/or service of the Bank.

- From publicly available sources such as, for example, data from publicly available services.

A precondition for any collection of personal data is the existence of an appropriate legal basis in accordance with the Law.

The Bank collects and processes the following categories of personal data – the overview is given comprehensively in relation to different purposes of processing:

- Data contained in contracts with Clients and application forms of Potential Clients – name and surname, personal identification number, name of one parent, residential address, citizenship, identification document number, place and date of issuance of identification document, country of birth, telephone number (fixed, mobile), address for delivery of mail, contact data, data on the manner and history of payment for services (amounts of debt, existence of a standing order, current account number, etc.), data from the account specification, etc.
- Financial data – data on earnings, other household income, data on other accounts and liabilities, data from the Credit Registry of the Central Bank of Montenegro, account number, card number, batch number, number of insurance policy, to which the data refer, data on tax residency and tax identification number, etc.;
- Property data (for certain types of placements) – real estate and movables owned by the person to whom the data relate;
- Special type of personal data – political affiliation (official status), disability data (to determine a person's income);
- Information about the spouse – data on the employment of the spouse, number of children, number of household members;
- Data on related parties – connection on the basis of management function, connection on the basis of kinship and other connections in accordance with the law;
- Data necessary for credit products – activity, data on the employer, including employment contract, credit history, previous use of banking products, and similar;
- Data on visits to our internet portals and information provided by Clients and / or Potential Clients by filling in the appropriate forms on our website, including but not limited to: name, surname, address, mobile phone number, landline number and email address;
- Mobile Device specific data
 - Geo-Location Information - we may request access or permission to and track location-based information from your mobile device, either continuously or while you are using the mobile application, to provide location-based services. If you wish to change our access or permissions, you may do so in your device's settings.
 - Mobile Device Access - we may request access or permission to certain features from your mobile device, including your mobile device's storage. If you wish to change our access or permissions, you may do so in your device's settings
 - Push Notifications - we may request to send you push notifications regarding your account or the mobile application. If you wish to opt-out from receiving these types of communications, you may turn them off in your device's settings.
- Information contained in the records on communications and correspondence in situations of establishing contact by the Client, Potential Clients and other natural persons, including recordings of conversations with the Contact Center, written or electronic communication;
- Data of Clients, Potential Clients and / or other natural persons from surveys used for research purposes, if the persons wish to be surveyed;
- Information that the Bank collects and processes for the purposes of direct marketing and profiling, based on the freely given consent of the data subject;
- Other personal data for which there is a legal basis for their processing in accordance with the law.

CKB Bank uses cookies on its websites, the purpose of which is to be able to provide the most complete service possible to the visitors of its websites.

CKB Bank treats all data transferred to it over the Internet using the same level of protection as if they were transferred to it using any other channel.

III.2. PURPOSES OF THE PERSONAL DATA COLLECTION

The CKB Bank processes the personal data of the data subject only when such processing is lawful. Processing is legal in the following cases:

1. Processing is necessary for the execution of the contract concluded with the data subject or in order to take action at the request of the data subject prior to the conclusion of the contract.
2. Processing is necessary in order to comply with the applicable legal regulations according to which the Bank is obliged to act, especially those that regulate banking operations and the implementation of payment operations services, as well as European legislation, primarily the obligation to report, check clients (prevent money laundering) and risk management. Based on a written request based on applicable legal regulations, the Bank is obliged to provide access to certain personal data of the Client/data subject to the competent state bodies (eg courts, police, etc.) in certain situations.
3. Processing is necessary in order to achieve the legitimate, law-based interests of the Bank or a third party, except when those interests are stronger than the interests or fundamental rights and freedoms of data subjects that require protection of personal data, especially if the data subject relations are minors.
4. The data subject has given consent for the processing of his / her personal data for one or more specially specified purposes, whereby that consent must be provable and voluntary, written in easy-to-understand language and the data subject has the right to withdraw his consent at any time.
5. Processing is necessary for the vital interests of the data subject or another natural person.
6. Processing is necessary for the purpose of performing activities in the public interest or exercising the legally prescribed powers of the Bank.

III.3. AUTOMATED PROCESSING

Decision-making based on automated data processing, including profiling, is carried out in accordance with:

1. applicable laws;
2. fulfillment of contractual obligations;
3. with the explicit consent of the data subject;
4. the legitimate interests of the Bank.

In accordance with the Law, the Bank enables data subjects to exercise the right to object to automated processing, including profiling. The complaint can be filed either in relation to the initial or further processing, at any time and free of charge.

III.4. RIGHT ON ACCESS TO PERSONAL INFORMATION

Only employees of the Bank, as well as hired associates have access to personal data in accordance with the tasks they perform on the basis of appropriate authorizations determined by the Bank and only to the extent necessary, with the obligation to act in accordance with the Bank's regulation which relates to personal data protection.

Personal data are available to third parties outside the Bank only in the following cases:

1. If there is a legal obligation or explicit authority under the law (eg a court request);
2. If a third party or subcontractor (processor) is engaged to perform certain tasks, whereby that processor acts exclusively in accordance with the order of the Bank, and the Bank ensures all data protection measures as if it performs these tasks independently;
3. Affiliated companies of the Bank provided that there is a legal basis for such transfer or access (consent of the person or legitimate, law-based interest);
4. If the data need to be forwarded for the purpose of performing the contract;
5. Other persons outside the Bank for whom there is the explicit consent of the data subject.

As a rule, the Bank processes your personal data in Montenegro, and exceptionally, the Bank may process this personal data in other countries or international organizations in accordance with the Law on Personal Data Protection.

III.5. PROTECTION OF THE PERSONAL DATA

Personal data are treated as a business secret of the Bank and are accordingly classified as confidential. In accordance with their classification, adequate protection measures are applied to them, which protect this data from injury, unauthorized access, accidental loss, destruction, damage, and any other security threat. For these purposes, technical and organizational measures are applied, such as control of access rights, establishment and implementation of information security policy and other related internal acts, establishment of segregation of duties, establishment and enforcement of confidentiality and compliance with the law of all third parties entitled to access personal data in the Bank's information system, application of methods for monitoring access and activities in information systems, as well as application of software solutions for the protection of information resources.

In the event of a breach of personal data that results or may result in accidental or intentional destruction, loss, alteration or unauthorized disclosure of personal data during their processing, which may pose a high risk to the rights and freedoms of data subjects, the Bank shall immediately upon learning of such violation, without undue delay, notify the Agency for Personal Data Protection and Free Access to Information and the data subject in a clear and understandable manner with a description of possible consequences and a description of measures taken. In the event of a breach of personal data, the Bank shall immediately take appropriate measures to prevent further damage to the rights and freedoms of the data subject and to reduce the consequences of that breach.

III.6. DATA SUBJECT'S RIGHTS

Clients, Potential Clients and other persons to whom personal data relate referred as Data Subject may exercise the following rights:

III.6.1. The right to access personal data

The applicant for the exercise of this right has the right to obtain information on the existence of processing of personal data relating to him, the purpose of processing, the type of personal data being processed, recipients or categories of recipients personal data are disclosed or may be disclosed, on retention periods, on the existence of the right to request correction or deletion of personal data, ie the right to limit the processing of such data, on the existence of the right to file a complaint.

III.6.2. The right to correction of personal data

The right to request the correction of inaccurate personal data, as well as the right to supplement incomplete data.

III.6.3. The right to restrict the processing of personal data

In the cases when the accuracy of personal data is disputed, the Bank will temporarily limit the processing for a period sufficient to verify the accuracy of personal data and when there is no legal basis for the processing of personal data, and the data subject opposes the deletion of data in order to submit the realization or defense of legal claims.

III.6.4. The right to object

This right refers to the right of a person to submit at any time an objection to the Bank on the legality of the processing of his / her personal data established on the basis of the appropriate legal grounds for processing.

III.6.5. The right to erasure ("right to be forgotten")

This right may be exercised in cases when the personal data have been processed illegally or there is no legal basis for the processing.

III.6.6. The right of a person to data portability

The right of a person to data portability means the right of a person who has submitted his personal data to the Bank in a structured, commonly used and electronically legible format, received by the Bank, as well as the right to transfer such data from the Bank to another controller. consent, is performed on the basis of a contract or in accordance with the Law on Personal Data Protection, and if the processing is performed automatically.

III.6.7. The right to revoke consent

The right to revoke consent may be exercised in anytime. The consent for the processing personal data given by the data subject is voluntary and may be withdrawn at any time.

III.7. EXERCISING DATA SUBJECT'S RIGHTS

Data subjects can exercise rights regarding the personal data that the Bank processes in all branches. All additional questions related to the processing of personal data, as well as questions related to the exercise of rights, Data subjects can send to:

E-mail: compliance@ckb.me.

Postal address: Crnogorska komercijalna banka a.d. Podgorica, Compliance Department, Bulevar Revolucije No. 17, 81000 Podgorica.

III.8. FILING A COMPLAINT TO THE SUPERVISORY BODY

The supervisory body for the protection of personal data in Montenegro is the Agency for Personal Data Protection and Free Access to Information (<https://www.azlp.me/me/kontakt>).

The person to whom the personal data refer has the right to file a complaint to the Agency if he / she considers that the processing of his / her personal data by the Bank is contrary to the provisions of the Law.

The data subject has the right to judicial protection if he considers that, contrary to the Law, the controller or processor has violated the right prescribed by the Law by processing his personal data.

IV. CLOSING PROVISIONS

This Policy shall become effective on the day of its adoption by the Management board with the consent of the Supervisory Board and shall become applicable on the day of publication on the intranet portal of the Bank and website www.ckb.me of the Bank.

With the entry into force of this Policy, the provisions of the Data Protection policy from December 14, 2022 cease to apply.

V. HISTORY OF THE VERSION

Version:	Date of adoption:	Description of modification:
1.0	14.12.2022.	Data Protection Policy
1.1	28.11.2024	Data Protection Policy