PERSONAL DATA PROTECTION POLICY

MAY 2022

Level of classification	**RESTRICTED INFORMATION**
Name of information asset	***Data Protection Policy***
Owner	*Compliance and AML Department*
Disclaimer	This document is intended solely for the use of the individual or entity to whom it is addressed or upon the legal request of the authorities, and contains restricted information. If you are not an addressee or otherwise authorized to use this document, you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have accessed this material in error, please advise its owner and the Information Security Officer immediately, delete any locally stored copies and destroy any hardcopies of the document.

Domeniul funcţional al organizaţiei:	**Compliance**
Reglementare:	**Data Protection Policy**
Responsabil:	**Compliance and AML Department**

REVIEWS

No	Date of approval by the Board of Administration	Date of approval by the Bank's Managers	Enforcement date	Content of the modification	Decision of the Board of Administration
1	24.05.2018	-	25.05.2018	-	Board of Administration Decision no. 1/24.05.2018
2	21.11.2019	-	25.11.2019	-	Board of Administration Decision no. 8/21.11.2019
3	30.05.2022		31.05.2022		Board of Administration Decision no. 4/30.05.2022

CONTENT

1. PURPOSE OF THIS POLICY

This policy must be comprehensive, providing all levels of personnel guidance regarding the personal data protection norms in accordance with the applicable national legislation and in according with the EU Regulation 2016/679 European Parliament.

The purpose of the Personal Data Protection Policy is to establish the basic principles for storing, use, management, transferring, and availability of the personal data with the aim to protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

The personal data protection management framework shall take in consideration the following principles:

- **Processed lawfully, fairly and in a transparent manner**: the bank shall ensure that the personal data are processed lawfully, fairly and in a transparent, in respect with, but without limitation to the personal data of the employees, potential employees, clients, potential clients, and to any natural persons which the bank has a business relationship. The processing of the personal data by using fraudulent, unfairly and unlawfully is forbidden. Processing shall be lawful only if and to the extent that at least one of the following applies:
  (a) the bank has the data subject consent to the processing of his or her personal data;
  (b) 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;
  (c) processing is necessary for compliance with a legal obligation to which the bank is subject;
  (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
  (e) 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 controller;

- **Purpose limitation principle :** The Bank shall ensure that the personal data for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The perosnal data are not 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;
- **Data minimisation principle**: The Bank shall process personal data in a adequate, relevant and limited way to what is necessary in relation to the purposes for which they are processed
- **Data accuracy principle :** The Bank shall take all reasonable steps to ensure that personal data are accurate and the inaccurate data are erased or rectified without delay
- **Integrity and confidentiality principle**: The Bank shall use appropriate technical and organizational measures which ensured appropriate security of the personal data, including protection against accidental loss, destruction or damage;
- **Accountability principle :** The Bank shall be fully responsable for processing of the personal data performed in its activities, including in case of transfering to the third parties, shall ensure that the principles regarding personal data processing and shall take all the necessary measures to demonstrate compliance with.

This policy may be complemented by guidelines, technical standards, job aids and procedures to help implement it and to ensure that the objectives of this policy are being met in full at every level and throughout the entire organization.

Therefore, The Data Protection Policy thereby addresses all employees of ProCredit Bank, as well as all third parties contractually bound to the Bank's business operations. All staff is hereby deemed responsible to put this policy and its supplementing guidelines into practice in their particular field of work.

2. DEFINITIONS

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;

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;

Restriction of processing - means the marking of stored personal data with the aim of limiting their processing in the future;

Pseudonymisation- means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Filing system - means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis

Controller - ProCredit Bank SA alone or jointly with others (natural or legal person, public authority, agency or other body), determines the purposes and means of the processing of personal data

Processor - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Recipient- means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or

Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Third party - means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;

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;

Personal data breach - means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Supervisory authority- means The National Supervisory Authority For Personal Data Processing.

3. SCOPE

This policy applies to all employees, trainees, and temporary staff from all locations and branches/agencies as well as to all other natural persons or legal entities affiliated or related to Procredit legitimate business purposes and processes that are using Procredit Bank S.A.

The policy also applies to all information carriers and systems used for legitimate business purposes of the Bank. It covers any information, which include personal data, no matter its type, storage support, method of creation, and transmission, such as paper based documents, electronic information or verbal expressions and conversations business or work related.

The aims of this policy are described as follows:

- Defining the framework for the Bank to manage the personal data;
- Identification of all security risks for the organization and its information, including an indication of the effects and costs associated with these risks;
- Illustration of the effects of data protection incidents on the critical business processes;
- Fulfillment of the security requirements resulting from legal and contractual stipulations.

The strategy to achieve an adequate level of compliance of the internal processes, which involved processing of the personal data, is to define and update this policy in line with the applicable legislation and business strategy development, to identify the relevant risks associate to inadequate personal data processing and to propose appropriate measures to comply with the purpose of this policy.

4. DATA PROTECTION OFFICER (DPO)

4.1 Responsibilities of the Data Protection Officer

- to inform and advise the Bank or the processor and the employees who carry out processing of their obligations pursuant to the data protection provisions;
- to monitor compliance with applicable legislation regarding data protection provisions of the Bank or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation, and to consult, where appropriate, with regard to any other matter.
- presents to the directors of the Bank, in order to approve, at the beginning of each year, the Work Plan of the Data Protection Officer for the current year;
- presents annually to the directors of the Bank the proposal for carrying out the bulk anonymization process;

- prepares and coordinates together with the Banking Applications Support Department the annual process of bulk anonymization of personal data;

In the performance of his/her activities stipulated in the job description, the data protection officer shall take in consideration in a proper manner to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

4.2 Reporting

Data Protection Officer reports to the Management of the Bank as following:

- ad-hoc reporting, in case of deficiencies in the process of data processing and in case of security incidents. In order to assess the findings, Data Protection Officer shall request relevant information from the departments involved in the security processes regarding personal data (IT department, the departments involved in the operational activities, audit department, risk management department) in order to prepare a finding report. This report shall mandatory include the following information: a description of the situation, the eventual risks generated, and the measures has been taken / shall be taken for mitigation of the deficiencies and proposal for a final resolution. This report shall be submitted to the Head of Compliance and AML Department and Bank's management.
- Quarterly reports to the Operational Risk Committee. The reports shall mention the situation of personal data security incidents related to the data protection related to the previous quarter, the final resolution submitted by the data protection officer, the measures agreed and the proposals in order to improve;
- Bi-annual reports to the Compliance Management Committee. The reports will include the analysis of the clients to be anonymised in the bulk anonymization process and the overview of the DPO activity for the last 6 months.

5. INFORMING AND TRINING STAFF

When hiring staff, the Bank will provide candidates with informative material on their obligations regarding compliance with the regulations in force on the personal data protection. Moreover, the Bank shall request a document signed and sealed by the candidate confirming that he/she has correctly and fully informed about the aspects of this policy

In order to avoid incompliance with the present policy and applicable legislation, it is considered necessary at the level of the institution, that all the employees to have adequate training in personal data protection requirements.

Trainings can be done both by attending training sessions such as seminars, as well as by providing / distributing educational materials through the e-learning platform.

In accordance with the provisions of present policy in the field, for categories of staff whose professional activities include processing of the personal data, face-to-face training sessions must be ensured at least once a year.

As well, all new employees are given an introductory course on how basic information on personal data protection provisions are brought to their attention

The responsibilities related to staff training belong to Data Protection Officer, which will also conduct staff assessment during training.

The staff evaluation will be carried out by conducting tests in order to check the employees' knowledge of personal data protection. Testing will be mandatory for all employees except for the following categories:

- Bank directors;
- administrative staff (secretaries, drivers, cleaners).

Testing will take place annually in the fourth quarter through the eLearning platform, after going through the material specifically prepared for this purpose. In exceptional cases, if at the end of the testing period there will be employees who could not take the test, additional testing sessions can be organized at the beginning of the following year.

6. RECORDS OF PROCESSING ACTIVITIES

The Bank shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
- the purposes of the processing;;
- a description of the categories of data subjects and of the categories of personal data;;
- the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;
- where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) EU Regulation UE 2016/679 the documentation of suitable safeguards
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of the technical and organizational security measures

The Bank, and, where applicable, the processor's representative, shall maintain a record of all categories of processing activities carried out on behalf of the Bank containing:

- the name and contact details of the processor which acting on behalf of the Bank, and, where applicable, of the controller's or the processor's representative, and the data protection officer
- the categories of processing carried out on behalf of the Bank
- where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
- where possible, a general description of the technical and organizational security measures

The records shall be in writing, including in electronic form. The Bank shall make the record available to the supervisory authority on request

7. SECURITY OF THE PERSONAL DATA

The Bank shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate;

- the pseudonymisation and encryption of personal data;
- anonymization of data when they have reached their retention period according to the Bank's nomenclature and the legislation in force by conducting an anonymization process once a year;
- deletion of personal data within a maximum of 6 months in the case of persons for whom the contracting process has not been completed;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed

The Bank shall adhere to the CODE OF CONDUCT OF THE ROMANIAN BANK ASSOCIATION REGARDING PERSONAL DATA PROTECTION, at the time of its finalization and implementation at the level of the Romanian banking system.

8. REGUESTS OF THE DATA SUBJECT REGARDING ACCES, RECTIFICATION, ERASURE, RESTRICTION OF PROCESSING AND PORTABILITY

8.1 Right of access by the data subject regarding the personal data processed by the Bank

In accodance with the applicable legislationm, the Bank shall provide to the any corserned person through official internet webpage and through other communication channels used by the Bank, the information regarding contact data of the Data Protection Officer.

The data subject can obtain from the Bank, through Data Protection Officer, confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;;
- the categories of personal data concerned;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the Bank rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source;
- the existence of automated decision-making, including profiling if it is the case
- in case the personal data are transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards according to the applicable legislation;

The subject data can request a copy of the personal data undergoing processing Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form

8.2 Rectification and erasure

The data subject shall have the right to obtain from the Bank without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement

The data subject shall have the right to obtain from the Bank the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent, in case the collecting and proccesing is based on the data subject consent
- the data subject objects to the processing pursuant and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for direct marketing purposes
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the Bank is subject;

The Bank, through Data Protection Officer, shall have the rights to reject the request if the processing is neccessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or Member State law to which the Bank is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Bank;
- for the establishment, exercise or defence of legal claims.

8.3 Restriction of processing

The data subject shall have the right to obtain from the Bank restriction of processing where one of the following applies:

- the data subject contests the the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the Bank no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to the Bank's processing rights and the Bank is in the verification period whether has the legitimate grounds for processing
- The data subject who has obtained restriction of processing shall be informed by the Bank before the restriction of processing is lifted

The Bank shall communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The Bank shall inform the data subject about those recipients if the data subject requests it.

8.4 Data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to the Bank, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- the processing is based on consent or on a contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means;

The data subject shall have the right to have the personal data transmitted directly from the Bank to another controller, the Bank shall proceed where technically feasible

9. INFORMATION / NOTIFICATION IN CASE OF PERSONAL DATA BREACH

9.1 Notification to the Data Subject:

- the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, and the Bank, through the Data Protection Officer, shall communicate the personal data breach to the data subject without undue delay in a clear and plain language the nature of the personal data breach and contain at least the information and the measures which have been taken by the Bank. The notification shall be sent not later than 72 hours. Where the notification is not made in accordance with the present paragraph, the Bank's notification shall be accompanied by reasons for the delay.

- the decision regarding the notification of the data suject shall be taken basen on assesment performed by the Data Protection Officer together with other responsable persons ("Emergency Response Team")) which shall contain:

- If there are implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, (e.g encryption)
- The Bank has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize;
- it would involve disproportionate effort

9.2 Notification to the supervisory authority

- in the case of a personal data breach, the Bank shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not possible to respect the deadline, it shall be accompanied by reasons for the delay.

- The notification shall provide at least the following information:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned ;
- communicate the name and contact details of the data protection officer ;
- describe the likely consequences of the personal data breach ;
- describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

9.3 The Security Incidents (DP) Register

The Bank shall maintain, through the Data Protection Officer, an Security Incidents (DP) Register regarding data protection in electronic format in which shall be recoded all personal data security breaches together with all the documents of the respective cases.

10. TRANSFER OF THE PERSONAL DATA

Considering that in the normal course of business the Bank initiates agreements which may have an impact on personal data, before initiating such agreements, the Data Protection Officer shall verify and endorse the irrespective document from national legislation and European perspective regarding personal data protection and in particular on the relevant provisions regarding the transfer of the personal data.

11. REVIEWS OF THIS POLICY

A comprehensive review of this policy in all parts must be undertaken on an annual basis by the Head of Compliance and AML Department based on the feedback received from the Data Protection Officer.

This policy is considered an auditable unit and therefore its implementation subject to the overall plans of internal and external audit.