PERSONAL DATA PROTECTION

POLICY

Version: 1 | Ref: POL/DC/004/V01

Effective Date: 11/03/2022

Security Classification: **PÚBLICO**

CONTENTS

1 GENERAL PROVISIONS

1.1 PURPOSE AND SCOPE

The purpose of the current Policy is to disclose to stakeholders information on BFA's personal data processing activities, in accordance with Law n.º 22/11 dated 17th June (hereinafter the Personal Data Protection Law or PDPL), which introduces regulatory requirements on the protection, confidentiality and privacy of citizens in the processing of personal data.

The Personal Data Protection Policy is intended for all BFA's staff members and the general public, including customers, suppliers and third parties.

1.2 LEGAL, REGULATORY AND NORMATIVE FRAMEWORK

The current document addresses the following Legislation, Regulations and Standards:

Table 1— Legislation, Regulation and Standards addressed

NAME	CLAUSE
Law n.º 22/11 dated 17th June – Personal Data Protection Law	_

On table 2 - In References are listed the documents referred to in this document:

Table 2— References

NAME	VERSION
n/a	n/a

On Table 3 – Relevant Internal Regulations – are listed the Relevant Internal Regulations for the subject regulated in this document, available on the Bank's public website and on the internal channels provided for that purpose.

Table 3 — Relevant Internal Regulations

NAME	VERSION
Code of Conduct	2019 version

1.3 DEFINITIONS AND ABBREVIATIONS

The key terminology used in the current Policy is detailed below:

1.3.1 ABBREVIATIONS

- **DPA -** Data Protection Agency
- **DPO -** Data Protection Officer
- **PDPL** - Personal Data Protection Law

1.3.2 DEFINITIONS

- **Data Protection Agency (DPA) –** The national authority empowered to regulate, supervise and oversee personal data protection. The Angolan Data Protection Agency (DPA) was created under Presidential Decree n.º 214/16 dated 10th October.
- **Personal Data –** Any information, whatever its nature or medium, including image and sound, concerning an identified or identifiable natural person (data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to a combination of factors specific to his physical, physiological, mental, economic, cultural or social identity.
- **Recipient –** A natural or legal person, public authority or any other body to whom personal data are disclosed, whether it be a third party or not.
- **Data Protection Officer (DPO) –** A natural or legal entity, appointed by the personal data processing controller, based on the controller's internal structure for data processing and considering the periodic assessment of compliance subject matters. A Directorate may be appointed and contact points may be nominated within it.
- **Data Protection System –** A group of actions or measures aimed at the implementation, management, control and monitoring of data protection at BFA, including the management of personal data breach risks.
- **Data Processing Controller –** The individual who alone or jointly with others determines the purposes and means of the processing of personal data.
- **Processing of Personal Data –** Any operation or set of operations which is performed upon personal data, whether or not by ring-fenced means, such as collection, recording, organisation, archiving, adjustment or modification, retrieval, consultation, utilisation, disclosure by transmission, by broadcasting or by any other means of making accessible, with comparison or interconnection, as well as blocking or destruction.
- **Personal Data Breach –** Breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to recorded personal data subject to any other type of processing.

1.4 REGULATORY REPEAL

Not Applicable.

1.5 ACCOUNTABILITY

The current Policy is reflected in the accountabilities identified in this document, in section 2.8 - Governance Model.

1.6 OMISSIONS

The cases of regulatory omission must be addressed to the Data Protection Officer prior to the adoption of any measures, through the contacts mentioned in subsection 1.8.

1.7 NON-COMPLIANCE

The breach of the provisions laid down in this document shall be subject to analysis by BFA's Compliance Department (CD) and, whenever justified, by BFA's Audit and Inspection Department (AID).

1.8 CONTACTS

Any queries regarding with the contents of this document should be addressed to:

Email address of the Data Protection Officer: bfa.proteccao.dados@bfa.ao

2 CONTENT REGULATORY COMPLIANCE

2.1 INTRODUCTION

BFA guides its business operations in accordance with a set of principles for data protection and has implemented the appropriate security measures to guarantee the rights of the data subjects, in compliance with the stipulations of its own regulations and with regard for the rights enshrined in the Constitution of the Republic of Angola.

2.2 ENTITY RESPONSIBLE FOR DATA PROCESSING

The entity responsible for the processing of personal data is BFA - Banco de Fomento Angola, SA, with head office at Rua Amílcar Cabral, n.º 58, Maianga, Luanda.

2.3 PROCESSED DATA

The personal data processed by BFA are those collected within the framework of the pre-contractual, promotional, commercial or employment relationships developed with customers, suppliers, counterparties, staff members and within the scope of applicable legal and regulatory obligations.

BFA processes personal data necessary for (I) the conclusion, execution and management of agreements, in which the data subject is a party, or in pre-contractual proceedings at the request of the data subject; (II) the safeguard of its legitimate interests or those of third parties; (III) to ensure compliance with various legal obligations. (IV) Additionally, BFA may perform other processing of personal data when it has obtained the prior, unequivocal, free, express and informed consent of the data subject.

2.4 DATA PROTECTION PRINCIPLES

BFA commits to act in accordance with the principles laid down in the Personal Data Protection Law, collecting data in a lawful, transparent and proportionate manner, as well as in relation to the Personal Data processing, stating the purpose of the collection, and guaranteeing its accuracy and appropriate retention period.

2.4.1 TRANSPARENCY

The processing of personal data is carried out in a transparent manner, in strict respect for the principle of privacy, and the rights of access, information, rectification, cancellation and opposition are guaranteed to the data subjects.

2.4.2 LAWFULNESS

The processing is carried out lawfully (there is a legitimate basis for it) and fairly, in accordance with the principle of good faith.

2.4.3 PROPORTIONALITY

Only personal data that is appropriate, relevant and not excessive in relation to what is necessary for the purposes that justify its collection and processing shall be collected and processed.

2.4.4 PURPOSE

Data is collected only for legitimate and explicit purposes, communicated at the time of collection, and is processed only with the express consent of the data subject or under other conditions provided by law.

Annex I of this document identifies the purposes envisaged by BFA for the collection of personal data.

2.4.5 VERACITY

Appropriate measures and processes are in place to guarantee the accuracy and veracity of the data subject to processing, and it is ensured that any inaccurate or incomplete data is rectified or deleted.

2.4.6 LENGTH OF THE RETENTION PERIOD

Personal data shall be kept in a manner which permits identification of data subjects for no longer than is strictly necessary period for the purposes for which the data were collected or processed and shall subsequently be erased or made anonymous. Personal data are only kept for longer periods for historical, statistical and criminal investigation and national security purposes with the authorisation of the Data Protection Agency (DPA).

2.5 DATA PROTECTION REQUIREMENTS

BFA undertakes the processing of personal data in order to meet the requirements of confidentiality and integrity, thus ensuring their security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, with the adoption of appropriate technical and organisational measures:

- Personal data is stored using secure and up-to-date applications for this purpose;
- Access to personal data is controlled and limited to authorised personnel only;
- The necessary security mechanisms are implemented to prevent unauthorised access and sharing of data;
- Data is deleted in a manner that ensures it is unrecoverable.

2.6 DATA SUBJECTS' RIGHTS

BFA ensures that data subjects may exercise their rights under the LPDP, as set out below.

Data subjects may exercise these rights through the following channels:

- At BFA branches by written communication or by filling in data forms.
- E-mail: bfa.proteccao.dado@bfa.ao

2.6.1 RIGHT TO INFORMATION

For the exercise of this right, BFA has the duty to provide information to the data subjects on: i) the purposes of the processing; ii) the recipients or categories of recipients; iii) the obligatory or optional nature of the reply, as well as the possible consequences of not replying; iv) the existence and conditions of the right of access and the right to rectify, update, eliminate and oppose; v) the consequences of collecting the data without the data subject's consent or, in the event of his incapacity, by his legal representative; vi) other information necessary to guarantee the lawful processing of such personal data.

2.6.2 RIGHT OF ACCESS

Whenever the data subject requests it, he/she shall be given access to his/her personal data or information relating to their processing (purposes, data categories, recipients), subject to any exceptions provided for by law.

2.6.3 RIGHT OF OPPOSITION

The data subject may object to the processing of their personal data, subject to the exceptions provided for by law.

2.6.4 RIGHT TO RECTIFY, UPDATE AND DELETE

BFA assures the data subject the right to rectify, update and delete their personal data, in situations where these are found to be incomplete or inaccurate, with exceptions provided for by law.

Namely, this right cannot be exercised in the following situations:

- Legal obligation or competent authority that forces the blocking and/or retention of the data for a certain period of time;
- There is a proven legitimate interest of BFA in the conservation of the data;
- For the purposes of criminal investigation;
- In the case of credit and solvency data, as long as the credit situation of the holder has not been settled and the time limits applicable to the credit relationship have not elapsed.

2.6.5 AUTOMATED INDIVIDUAL DECISIONS

The data subject shall have the right not to be subject to decisions based on automated processes intended to evaluate certain aspects of his or her personality, in particular his or her professional ability, creditworthiness, reliability or conduct. This right does not apply in the following situations:

- Where the processing occurs in the course of the signing or performance of an agreement and under the condition that your request to sign or perform the agreement has been granted;
- Where there are appropriate measures to safeguard your legitimate interests, in particular your right of representation and expression.

2.7 DOCUMENTARY MODEL

The current Personal Data Protection Policy is supported by a set of internal documents of various levels which, as a whole, provide guidelines in information security management and personal data protection, formalise BFA's regulatory framework and the underlying approval processes.

2.8 GOVERNANCE MODEL

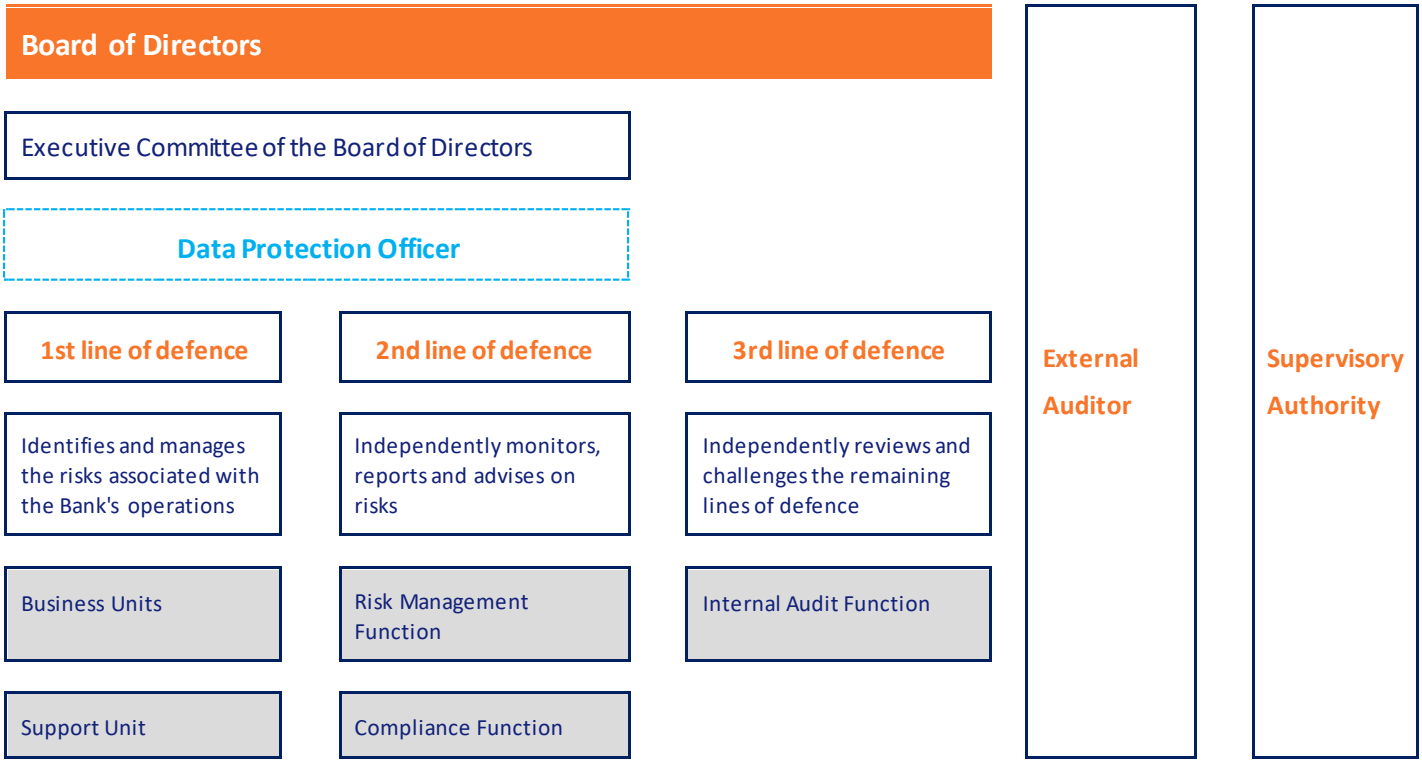
The governance model adopted in BFA's Personal Data Protection System, described below, was structured in accordance with BFA's Corporate Governance Model, taking into consideration, in particular, the following structuring principles:

- The Board of Directors is collectively responsible for maintaining and overseeing an appropriate governance of Personal Data Protection;

- The Institution adopts an organisational structure that complies with the principle of separation of functions, ensuring a clear separation between the responsibilities of the business and support areas, supervisory areas and those areas of independent review;
- In addition to these lines of defence, the organisation is subject to inspection by external auditors and supervisory authorities.

The principle of separation of functions is operationalised according to the three lines of defence model depicted in Illustration 1.

Illustration 1— Organisational Model of the Personal Data Protection System



2.8.1 FIRST LINE OF DEFENCE

The first line of defence is carried out by the BFA Departments (Front, Middle and Back Office), which are primarily responsible for identifying, assessing, controlling and reporting the personal data protection risks associated with their areas of activity in alignment with the applicable regulations. It is generally incumbent upon them to:

- To promote high quality standards and best business practices aligned with BFA's strategy for personal data protection, regulation and corporate culture;
- To implement the policies, regulations and procedures as well as the requirements and action plans aimed at the appropriate protection of personal data and associated risk management;
- To report any events that may compromise data protection.

Also included in the first line of defence are the Information Security Officer, the Physical Security Officer and the Business Continuity Officer, as support bodies for the risk management departments, including those related to personal data protection.

2.8.2 SECOND LINE OF DEFENCE

The second line of defence bodies perform their function independently and have authority and autonomy, reporting directly to the Board of Directors. The scope of their activity includes monitoring the implementation of effective risk management practices and Internal Controls methodologies of Compliance, as well as providing support and assistance, of a consultative nature, to the BFA structures in the first line of defence.

Furthermore, they are responsible for testing and assessing adherence to regulations, policies and procedures, maintaining integrity standards aligned with the principles, guidelines and risk appetite undertaken, systematically and timely reporting to the Board of Directors the results of their analysis in relation to the level of compliance.

The second line of defence includes the Data Protection Officer as the individual responsible for compliance with data protection at BFA.

2.8.3 THIRD LINE OF DEFENCE

The third line of defence is performed by the Internal Audit Function, which is independent, has authority, autonomy, and reports directly to the Board of Directors. Its responsibility is to assess the efficiency and effectiveness of BFA's Data Protection System, and to identify shortcomings and opportunities for improvement, systematically reporting the results of these assessments to BFA's Executive Committee of the Board of Directors and to the Audit and Internal Control Committee.

2.9 GOVERNANCE BODIES

2.9.1 BOARD OF DIRECTORS (BOD)

BFA's Board of Directors is the ultimate duty holder body in charge of data protection management and risk management of the Institution, performing its duties and obligations in accordance with the provisions set out in its internal regulations, and within this scope, it is particularly responsible for the following:

- To promote a culture of compliance with regard to data protection;
- To lay down the strategy, targets and guidelines with regard to the protection of personal data;
- To approve and review the current Personal Data Protection Policy;
- To ensure within BFA's organisational structure, the existence of a Data Protection Officer, duly trained and with the resources and means necessary for the performance of his/her duties;
- To establish the risk appetite for data protection infringements or breaches, within the framework of the approval and review of the BFA Risk Appetite Statement (RAS).

2.9.2 EXECUTIVE COMMITTEE OF THE BOARD OF DIRECTORS (ECBOD)

The Executive Committee of the Board of Directors (ECBOD), under the terms of its internal regulations, is responsible for BFA's day-to-day management and primarily responsible for implementing risk policies and risk limits within the scope of personal data protection. For this purpose, it is responsible in particular for:

- To propose to the Board of Directors policies, strategic plans and budget within the scope of personal data protection;
- To implement the strategy and policies in the field of data protection, or delegate this function to structural bodies with the appropriate profile;
- To ensure the existence of structures, the provision of resources and the allocation of authorities necessary to achieve the objectives established for compliance with the legal and regulatory provisions on the protection of personal data and inherent risks;
- To ensure the monitoring of compliance with what is determined in BFA's data protection policies and, inherently, that BFA's structural bodies integrate this component at all times in the institution's processes;
- To guarantee the implementation of appropriate mitigation or corrective measures, whenever breaches to BFA's rules and regulations are detected, through this policy and related regulations;
- To report to the Board of Directors on a timely basis on the subject of data protection risk management that may generate legal risks, regulatory sanctions, financial or reputational losses.

2.9.3 DATA PROTECTION OFFICER (DPO)

The Data Protection Officer's duties are the following:

- To ensure that BFA operates in compliance with legal and regulatory requirements with regard to data protection;
- To support the top management bodies in setting the strategy, purposes and guidelines within the scope of personal data protection;
- To assist in the setting up and implementation of policies governing subject matters related to the protection of personal data;
- To support and guide the BFA management bodies with regard to the adoption of procedures and good practices, and to this purpose, it is particularly responsible for:
  - In liaison with the Compliance Function:
    - To promote training and awareness-raising to ensure adequate empowerment and integration of data protection principles as part of BFA's culture;
    - To provide guidance and assist in the establishment and implementation of processes and procedures resulting from the provisions laid down in the current Policy and related regulations;
    - To promote compliance with BFA policies, processes and procedures regarding the protection of personal data;
    - To support the analysis of background check operations, involving personal data, conducted by this function;
    - To support the adjustment of contractual clauses and terms of usage, when applicable.
  - To support BFA's structural bodies with risk management responsibilities in establishing the 'Key Risk Indicators' to ensure a better control and reporting of the main data protection risks identified, as well as their maintenance within the risk appetite stipulated by the Bank.
  - In liaison with the Bodies of the first line of defence:
    - In particular the ones in charge of technology management and information security, which should analyse and guide in an impartial way, the acquisition of technologies and all issues involving information security applied to data protection, including promoting the adoption of IT security measures;

  - To support the definition and implementation of an appropriate technical and organisational structure for risk management and incident management for the protection of personal data;
  - To support in carrying out the impact assessment of the personal data processed in order to comply with BFA's duties of prior consultation and notification to the national data protection supervisory authorities;
  - Derives from the previous sub-point, within the scope of the assessment on the exposure to the risks of data protection breaches and promote the implementation of appropriate mitigation measures aimed at its ongoing improvement;
- To promote the maintenance of a record on the processing of personal data and the related purposes and ensure that the legally and regularly foreseen measures are adopted, concerning the collection, retention, handling, including data transfer (when applicable), preservation and disposal of personal data;
- To draw up and report in a timely manner to the management bodies on BFA's performance with regard to data protection;
- To operate as the primary point of contact between BFA and the Data Protection Agency and other public authorities and, to this purpose, to collaborate, hold prior consultations and notify these authorities about the personal data processed by BFA ;
- To promote the dissemination and broad access of the information to the subjects of personal data, in particular on their rights, means and channels for exercising those rights.

2.9.4 COMPLIANCE FUNCTION

The BFA Compliance Department's Responsibilities as Data Protection Officer are as follows:

- To monitor corporate compliance and adherence to the current Policy and related regulations;
- To closely monitor the evolution of the regulatory environment and timely communicate changes to BFA's structural bodies with responsibilities in data protection management and risk management, while supporting the necessary adaptation of processes and procedures guaranteed by these bodies;
- To propose, where appropriate, to the Executive Committee of the Board of Directors (ECBOD) the adoption of new procedures to ensure that BFA permanently complies with the applicable laws and regulations of the regulatory and supervisory authorities;
- To report, within its scope of activity, identified non-compliances and proposals for improvement;
- To promote training and awareness-raising on the provisions laid down in the current Policy and to foster a corporate culture in which the principles of data protection are an integral part of the institution's culture.

2.10 EXCEPTIONS

All exceptions to this document shall be duly documented and formally approved by the Board of Directors (BoD) and, if necessary, reflected in an update of the current Policy.

ANNEX 1 PURPOSES FOR THE PROCESSING OF PERSONAL DATA AT BFA

Table 4 – Purposes for the processing of personal data

PURPOSE	PURPOSE DETAILS
Products, services and sales communication	Communication or sale of new products or services Analysis and definition of consumer profiles Adaptation and/or development of new products or services Research and information processing
Customer Management and Service Delivery	Management of contacts, information, requests or complaints Management of invoicing, collections and payments Management of the financial service provided Call recording to prove business transactions and communications within the contractual relationship Call recording for monitoring the quality of information
Tax and Administrative Accounting Management	Accounting and invoicing Fees and commissions management Tax information including sending information to the relevant National Authority
Litigation Management	Judicial and Extrajudicial Collections Other Conflict Management
Fraud detection, revenue protection and audit	Detection of fraud and unlawful practices Revenue protection and control Management of credit or other risks Control, Audit and Investigations
Networks and Systems Management	Improvement of the networks and applicational tools and systems that support the Bank's services and products Monitoring
Compliance with applicable regulations and laws	Reply to judicial, regulatory and supervisory authorities Investigation, detection and prosecution of fraudulent or criminal events
Information Security Control	Logs and access management Backup management Security incident management
Physical Security Control	Video surveillance in the Bank's premises

DOCUMENTARY CONTROL

DOCUMENT PROPERTIES

Table 5— Document Properties

DOCUMENT PROPERTIES			
Name	Personal Data Protection Policy		
Type	Policy	**Classification**	PÚBLICO
Version	1	**Reference**	POL/DC/004/V01
Author	BFA - Organization and Quality Department (OQD) and Compliance Department (CD)	**Approved by**	BFA's Board of Directors (BOD)
Approval Date	04/03/2022	**Effective Date**	11/03/2022
Publication Date	11/03/2022	**Review Date**	11/03/2025
Document Holder	Data Protection Officer (DPO)		
Target Audience	BFA Staff Members and General Public		
Availability	This document is updated on the Bank's intranet at: • Regulation | Compliance | Policies | **Personal Data Protection Policy**		
Main amendments	First version		

VERSIONS RECORD CONTROL

Table 6— Versions Record

VERSION	APPROVAL DATE	APPROVED BY	EFFECTIVE DATE	MAIN AMENDMENTS
1	04/03/2022	BFA's Board of Directors (BOD)	11/03/2022	First version