

## TABLE OF CONTENTS

1.   INTRODUCTION.....	2
2.   OBJECTIVES.....	3
3.   SCOPE OF APPLICATION.....	3
4.   REGULATORY FRAMEWORK. REGULATIONS AND APPLICABLE LEGISLATION.....	4
5.   GENERAL PRINCIPLES.....	5
6.   CRIME PREVENTION MODEL.....	6

## 1. | INTRODUCTION

- Banco BPI, S.A. (hereinafter "BPI", "Entity", "Institution" or "Bank") is a credit institution within the CaixaBank Group which carries out banking activities, including all ancillary, related or similar operations compatible with this activity and permitted by law, and which adopts, with the necessary adaptations, CaixaBank's corporate policies.
- CaixaBank has a Corporate Policy on Criminal Compliance which, with the necessary adaptations, is applicable to all the Group's entities, namely its subsidiaries, and which defines the fundamental principles of action in Corporate Criminal Management.
- Without prejudice to the above, but always conscious of BPI's desire to raise its standards of demand and transparency, combined with the need, on one hand, to strengthen its Policies and procedures to standardise them with the other CaixaBank Group entities and, on the other, to ensure the necessary compliance with the legislation and/or regulations specifically applicable in the Portuguese legal system, resulted in the drafting of this Policy.
- This Policy promotes the creation and implementation of a criminal prevention programme, applied across the entire Bank, capable of reducing the risk of crimes being committed by strengthening the duties of vigilance and control referred to in Article 11 of the Portuguese Criminal Code (hereinafter the "Criminal Code"), defining clear compliance procedures and adequate control mechanisms to prevent illicit and/or inappropriate conduct as well as BPI's criminal liability.
- Law no. 94/2021, of December 21, introduced changes to the Criminal Code, namely by expanding the list of crimes for which legal persons and equivalent entities may be held liable, expressly reinforcing their criminal liability in relation to some crimes, when committed:
  - a) in their name or on their behalf and in their direct or indirect interest by persons who occupy leading positions in them; or
  - b) by anyone acting in their name or on their behalf and in their direct or indirect interest, under the authority of said persons, as a result of a breach of their duties of supervision or control (Article 11(1) and (2) of the Criminal Code).
- In addition to the Criminal Code, there are other laws that recognise the criminal liability of legal persons, particularly the provisions of the following: the Securities Code (article 401); the General Regime for Credit Institutions and Financial Companies (articles 200 and 200-A); the General Regime for Tax Infringements (articles 3 and 7); Law 52/2003, of August 22, on combating terrorism (article 6); Law no. 20/2008, of April 21, on criminal liability for corruption offences in international trade and the private sector (article 4); Law no. 58/2019, of August 8, approving the Personal Data Protection Act (article 54); Law no. 83/2017, of August 18, on measures to combat money laundering and terrorist financing (article 159-A); the Labour Code approved by Law no. 7/2009, of February 12 (article 546); and Law no. 109/2009, of September 15, which approves the Cybercrime Law (article 9).
- In this context, this Policy aims to create appropriate systems for preventing and controlling compliance with the various applicable criminal provisions, with the aim of preventing BPI from incurring contingencies of this nature.

TABLE OF CONTENTS

## 2. | OBJECTIVES

The objectives of this Policy are the following:

- Conveying to all Employees and Members of BPI's Governing Bodies, as well as to Associated Persons<sup>1</sup> to whom the general principles of this Policy apply (with the necessary adaptations, in the case of Associated Persons, as they are not Employees of BPI), BPI's commitment to ensuring that its activity is based on respect for the law and regulations in force at all times, and the promotion and defence of its corporate values and principles of action set out in its Code of Ethics. Thus, in line with its ethical values, BPI firmly reiterates its intention to maintain a behaviour of strict compliance with and respect for the law, particularly in criminal matters.
- Establishing a general framework for the Bank's Criminal Prevention Model in accordance with current legal provisions and best practices. The Model comprises a set of measures aimed at preventing, detecting and reacting to possible criminal behaviour and identifies the risks and controls associated with them.
- Ensuring, in relation to Clients, suppliers, judicial bodies/entities and society in general, that BPI fulfils its duties to supervise and control its activity, establishing appropriate measures to prevent or reduce the risk of the commission of criminal offences, enforcing compliance with this Policy by all Employees and Members of the Governing Bodies and Associated Persons.

Additionally, BPI has defined:

- The risks associated with different types of crime which, in accordance with the Criminal Code and other related legislation, may be attributable to legal persons in Portugal, distinguishing, on one hand, crimes whose risk of possible commission, given the Bank's corporate purpose and normal activity, could have a serious impact on BPI's reputation and activity, and on the other hand, other legal types whose criminal relevance is more general in nature.
- The risks associated with types of crime which, although not attributable to legal persons, may still be relevant in the sector, given the activity carried out by BPI. Particularly, we find reference to crimes against the market, crimes relating to the defence of copyright and related rights and the prevention of and reaction to labour harassment.

[TABLE OF CONTENTS](#)

## 3. | SCOPE OF APPLICATION

- This Criminal Compliance Policy (hereinafter referred to as "the Policy") applies to all Employees and Members of BPI's Governing Bodies.
- For the purposes of applying the Corporate Criminal Compliance Policy, CaixaBank, among the companies that comprise the CaixaBank Group, establishes a division between two types of Entities:
  - a) **Perimeter entities**, those with the following characteristics: majority shareholding, permanent control and nature, solid structure and development of an activity related to CaixaBank's activity.
- Among the Perimeter Entities, the Corporate Criminal Management Committee shall define special treatment for companies considered significant, due to their criticality within the Group

<sup>1</sup> Natural or legal persons who maintain commercial/business relations, regardless of their nature, with BPI. Among others, intermediaries, agents, brokers, external consultants or other natural or legal persons contracted to supply goods and/or provide services (*outsourcers*).

and/or due to the existence of specific requirements given that they are entities subject to additional regulations to normal national and European banking regulations.

Due to this greater complexity, the Corporate Criminal Management Committee will set different reporting frequencies for these entities as compared to the other entities that comprise the Perimeter.

BPI has been classified by CaixaBank as a Perimeter Entity and is therefore required to report regularly to the Corporate Criminal Management Committee.

b) **Entities outside the Perimeter** are those which do not share any of the characteristics listed above.

- The general principles of this Policy shall also apply to all Associated Persons of BPI, including, specifically, intermediaries and agents acting in the name or on behalf of the Bank, whenever the circumstances of the specific situation so permit, to ensure effective compliance with the Law.

TABLE OF CONTENTS

#### 4. | REGULATORY FRAMEWORK. REGULATIONS AND APPLICABLE LEGISLATION

This Policy is subject to the applicable legislation and regulations in force, as well as any updates or revocations that may occur in the future. The following is a non-exhaustive list of the laws and/or other documents that comprise the regulatory context of this policy:

- Decree-Law no. 48/95, of March 15, approving the Portuguese Criminal Code and its subsequent amendments.
- Decree-Law no. 262/86, of September 2, approving the Commercial Companies Code, and its subsequent amendments.
- Decree-Law no. 486/99, of November 13, approving the Securities Code and its subsequent amendments.
- Law no. 20/2008, of April 21, establishing the criminal liability regime for crimes of corruption in international trade and private activity and its subsequent amendments.
- Decree-Law no. 298/92, of December 31, approving the General Regime for Credit Institutions and Financial Companies and its subsequent amendments.
- Law no. 15/2001, of June 5, approving the General Regime of Tax Infractions, and its subsequent amendments.
- Law no. 83/2017, of August 18, approving measures to combat money laundering and terrorist financing.
- Law no. 58/2019, of August 8, approving the Personal Data Protection Act.
- Law no. 109/2009, of September 15, republished by Law no. 79/2021, of November 24, approving the Cybercrime Law, transposing into national law Council Framework Decision no. 2005/222/JHA, of February 24, on attacks against information systems, and adapting national law to the Council of Europe Convention on Cybercrime.
- Decree-Law no. 109-E/2021, of December 9, which creates the National Anti-Corruption Mechanism and approves the General Regime for the Prevention of Corruption (RGPC).
- Law no. 93/2021, of December 20, establishing the General Whistleblower Protection Regime, transposing Directive (EU) 2019/1937 of the European Parliament and of the Council.

- Ordinance no. 155 155 B/2023, of June 6, declaring the definitive installation of the National Anti-Corruption Mechanism.
- US Foreign Corrupt Practices Act (1977).
- United Nations Convention against Corruption (2003).
- Rules of the International Chamber of Commerce to combat corruption (2005).
- UK Bribery Act (2010).

Furthermore, this Policy takes into consideration other national and international reference documents on criminal liability:

- ISO Standard 37001 for Anti-Bribery Management Systems.
- UNE Standard 19601 on Criminal Compliance Management Systems.
- UNE Standard 19602 on Tax Compliance Systems.
- ISO Standard 37301 on Compliance Management Systems.
- ISO Standards 37002 on Whistleblowing Management Systems.

[TABLE OF CONTENTS](#)

## 5. | GENERAL PRINCIPLES

This Policy and, consequently, the Criminal Prevention Model, are subject to the following principles:

- Acting in accordance with the legislation in force at all times, with the Code of Ethics, the applicable rules of conduct, as well as other internal regulations and policies.
- Promoting a corporate culture of prevention and intolerance towards the practice of illegal acts, as well as encouraging the application of ethical principles and responsible behaviour.
- Ensuring effective, permanent, and up-to-date control systems are always in place.
- Supervising the compliance of all actions and decisions adopted at BPI with the established internal rules and procedures, as well as the corresponding controls. In the case of Associated Persons, these actions and decisions are those defined and contractually agreed between the Parties.
- Ensuring the existence of adequate resources and means for the application of this Policy to prevent or detect possible criminal offences.
- Carrying out training activities that are appropriate and necessary, with sufficient frequency, to ensure that knowledge in this matter is updated and that a culture of business ethics and compliance with the law is developed.
- Informing all natural or legal persons within the scope of this Policy of their responsibility to monitor potentially illegal behaviour from a criminal perspective. Particularly to all those in charge of Employees or work teams, who will ensure that illegal behaviour is prevented and reported as soon as possible and diligently to the responsible bodies, as well as acting in accordance with the defined process as soon as they detect any behaviour that qualifies as a criminal offence.
- Always promoting a culture of compliance which, with the appropriate guarantees of confidentiality and protection for the whistleblower, favours the reporting of possible risks and/or irregularities at criminal level, through the channels established for this purpose.
- Investigating potential criminal offences as quickly as possible, guaranteeing in any case the rights of those involved in the investigation.

- Ensuring that the disciplinary sanctions foreseen for situations of possible internal violations related to criminal offences are disclosed, according to the Internal Policy and the legal provisions in force, in coordination with the area or areas especially competent in this matter.

TABLE OF CONTENTS

## 6. | CRIME PREVENTION MODEL

- In this context, it is therefore vital to ensure the existence of an organisational and management model for crime prevention, which includes an adequate control system, aimed at preventing and avoiding conduct that could constitute criminal liability for BPI.
- This Model includes the following main elements:
  - i. A body with autonomous powers of initiative and control to supervise the operation and fulfilment of the Prevention Model implemented. At CaixaBank and its Perimeter Entities, these functions are carried out by the Corporate Criminal Management Committee, as described in the previous section.
  - ii. The existence of a Representative of BPI's Corporate Criminal Management Committee who, in coordination with the Corporate Criminal Management Committee, is responsible for monitoring and supervising the operation of and compliance with the Prevention Model implemented.
  - iii. Identification of BPI's activities in which the crimes intended to prevent may be committed.
  - iv. Implementation of the organisational measures and procedures that materialise the decision-making process and the adoption and execution of BPI's decisions with a Criminal impact.
  - v. The existence of adequate resources to prevent the commission of the crimes they are intended to prevent.
  - vi. Obligation to inform those responsible for overseeing the operation of and compliance with the Prevention Model of all situations in which possible risks and non-compliance are detected.
  - vii. Existence of a system for detecting and reporting criminal offences, means for detecting and reporting possible criminal offences.
  - viii. Application of disciplinary sanctions for internal offences, in accordance with internal regulations and current legal provisions, in coordination with the area or areas especially competent in this matter.
  - ix. Periodic review of the Model and the introduction of possible changes when there are legislative, organisational, or business modifications and whenever justified.
- This Model has five (5) distinct phases, further developed in the Bank's internal regulations:
  1. **Prevention:** identification of behaviours that may imply a criminal risk for the activity of BPI and the CaixaBank Group and determination of applicable controls in this regard.
  2. **Detection:** identification or detection of possible criminal offences reported through internal channels and existing means.
  3. **Response:** intervention by the Representative of BPI's Corporate Criminal Management Committee in the event of indications or suspicions that a criminal offence has been committed at BPI, who will immediately develop strategies that, where possible, mitigate the damage or losses that may arise.

4. **Reporting:** communication and provision of information every six months by the Representative of BPI's Corporate Criminal Management Committee to the Corporate Criminal Management Committee. In addition, this Representative will also report to BPI's Management and Supervisory Bodies.
5. **Monitoring:** evaluation of the Model and its adaptation, both to changes in circumstances at CaixaBank, BPI and the other Perimeter Entities, and to changes in requirements in terms of criminal prevention by legal persons, given legislative, jurisprudential, and doctrinal developments. The Model may be subject to internal or external audits at least every three years to ensure it is periodically assessed.

[TABLE OF CONTENTS](#)