General principles of the Corporate Policy for the Prevention of Money Laundering and the Financing of Terrorism and managing Sanctions and International Countermeasures

29 April 2024

Table of contents

1. Introduction

1.1 Background

Caixabank, S.A. (hereinafter "CaixaBank"), as the parent company of the businesses that comprise its group (hereinafter, "Group" or "CaixaBank Group" interchangeably), is firmly committed to the prevention of money laundering and to countering the financing of terrorism (hereinafter, AML/CFT) and to complying with international sanctions programmes and financial countermeasures (hereinafter, "Sanctions"), actively promoting the application of the highest international standards in this regard.

Financial crime is a universal and globalised phenomenon that takes advantage of the removal of trade barriers and the internationalisation of the economy to manifest itself. The fight against this phenomenon requires and demands a coordinated response from the international community in general and the financial sector in particular, to avoid being used for illicit purposes inadvertently and involuntarily.

1.2 Concept of the risk of Money Laundering and Terrorist Financing and Sanctions

The following definitions are used to interpret and apply these Principles:

Money laundering

- The conversion or transfer of assets, knowing that said assets are the result of a criminal activity or from participating in a criminal activity, with the intent to shield or conceal the illicit origin of the goods or to help people who are involved in avoiding the legal consequences of their acts.

- The concealment or disguise of the true nature, origin, location, disposition, movement, or ownership of property or rights to property, knowing that such property originates from a criminal activity or involvement in a criminal activity.

- The acquisition, possession, or use of goods, knowing at the time they are received that they originate from a criminal activity or participation in a criminal activity.

- Participation in any of the activities mentioned in the paragraphs above, conspiring to commit said acts, attempts to perpetrate them and helping, instigating or advising someone to carry out or facilitate their execution.

Property from criminal activity shall be understood as all types of assets whose acquisition or possession originates in a criminal offence, whether material or immaterial, movable or immovable, tangible or intangible, as well as legal documents or instruments, regardless of their form, including electronic or digital, that prove ownership of said assets or give a right to them, including the amount of the amount defrauded in the case of crimes against the Public Treasury.

Money laundering shall be regarded as such even when the activities which generated the property to be laundered were carried out in the territory of another State.

Finally, it should be noted that the money laundering process usually entails the following phases:

1. **Placement or concealment**: Cash from criminal activities is introduced into financial circuits or exchanged for a different asset.

2. **Accumulation:** Making transfers or movements between different products or services in one or more jurisdictions in order to divide, accumulate, hide, transfer the amounts and deposit them in jurisdictions that are less stringent in terms of investigating the source of fortunes, or in accounts where the origin of the money appears legitimate, or engaging in other transactions that keep the real origin concealed.

3. **Integration:** Insertion of the capital into the financial system under the guise of legitimacy.

The companies of the CaixaBank Group may be used at any stage of the process described, primarily in the "placement" phase, meaning the necessary internal control measures must be adopted to manage this risk.

Terrorist financing

The provision, deposit, distribution, or collection of funds or goods, by any means, directly or indirectly, with the intention of using them or with the knowledge that they will be used, in whole or in part, to commit any of the terrorism-related crimes defined in the applicable criminal law.

Terrorist financing shall be regarded as such even where the supply or collection of funds or property were carried out in the territory of another State.

Programmes of sanctions and international financial countermeasures

Instruments of a political, diplomatic or economic nature used by countries and international or supranational bodies for the purpose of implementing restrictive measures that prevent violations of international law, human rights or civil rights and freedoms.

1.3 Goal

The goal of this document is to list the principles and premises that regulate the prevention of money laundering and combat the financing of terrorism (hereinafter AML/CFT) and Sanctions.

The purpose of these General Principles of the Corporate Policy on AML/CFT and Sanctions (hereinafter the "Principles") is to establish a framework of compliance in the Group that all companies must apply in the exercise of their activities, their business and their relations, both nationally and internationally, to

prevent money laundering and terrorist financing, and to comply with the various applicable international financial sanctions and countermeasures programmes.

2. Scope

These Principles are corporate in nature. Consequently, the principles of action defined are applicable to all CaixaBank Group companies that engage in any of the activities included within their scope. The governing bodies of these companies will take the appropriate decisions in order to integrate the provisions of these Principles, adapting, in keeping with the principle of proportionality, the governance framework to the characteristics of their governance bodies, committees and departments, and their principles of action, methodologies and processes to the contents described herein.

This integration may prompt, among other decisions, the company to approve its own policy. Approval will be required in companies that need to adapt the provisions of these Principles to their own circumstances, whether in terms of matter, jurisdiction or the relevance of the risk in the company. In this case, the compliance function at CaixaBank (Compliance Department), given its corporate nature, will ensure that these policies are consistent with the corporate policy, and consistency across the CaixaBank Group.

In addition, in those cases where the company's risk control and management activities are carried out directly by CaixaBank, whether due to the materiality of the risk in the company, for reasons of efficiency or because the company has outsourced the operational management of this risk to CaixaBank, the governing bodies of the companies concerned will be made aware of the existence of this corporate policy and its application to said companies.

3. Regulatory framework. Applicable standards and regulations

These Principles shall be governed by the content of the applicable regulations, as well as by those that modify or replace them in the future. Specifically, on the date of this writing, the regulations applicable to the Group's parent company are as follows:

- Act 10/2010, of 28 April, on the prevention of money laundering and the financing of terrorism.
- Royal decree 304/2014, of 5 May, approving the text of Act 10/2010, of 28 April, on the prevention of money laundering and the financing of terrorism.
- Act 12/2003, of 21 May, blocking terrorist financing.
- European Union regulations related to the application of the regulation on the prevention of money laundering.
- European Union regulations related to the application of international financial sanctions.
- Standards of international bodies, mainly represented by the Recommendations of the Financial Action Task Force (FATF).

In the case of companies or, where applicable, branches subject to foreign jurisdictions or complementary sector regulations, the policies and procedures that these companies develop will take into account, in addition to their own regulations, the obligations at the consolidated level contained in the regulations referenced above, as long as they do not contradict the specific requirements of the corresponding jurisdiction or sector regulations.

Finally, each Group company or, where applicable, branch, will develop the frameworks, standards, guidelines or procedures that are necessary for the proper implementation, execution and compliance of these Principles.

4. Management framework for AML/CFT and Sanctions

The main principles and standards that comprise the prevention framework that these Principles regulate are:

1. Risk assessment
2. Due diligence
3. Detection, control and examination of operations
4. Reporting suspicious transactions.
5. Screening sanctions lists and reporting matches
6. Document storage
7. Training
8. Consolidated risk management

4.1 Risk assessment

The Group companies' exposure to the risk of money laundering, terrorist financing and sanctions is directly related to the type of business or activity, the products marketed, the services rendered, the marketing channels, the types and characteristics of customers, and/or the jurisdictions in which they operate.

In order to maintain a suitable risk-based control and prevention framework, the Group's companies must be categorised by their risk level such that a higher level of supervision is applied to those companies, segments, channels, jurisdictions or products that pose a higher risk level.

4.2 Due diligence

The customer admission policy and due diligence measures may not, under any circumstances, represent a violation of rights in jurisdictions where the Group company carries out its activities.

The customer admission policy is dynamic and establishes a compliance framework in the Group that may vary based on the risk level of certain segments or activities, depending on their exposure to this risk at any given time. The admission policy must comply with international standards and the "Know Your Customer" principle (also known as KYC), with a particular emphasis on ensuring that the bank is always knowledgeable of the customer and their activities.

The Know Your Customer principle and due diligence policies will always apply a risk-based approach and ensure that the measures taken are appropriate to the underlying risk of money laundering, terrorist financing or sanctions.

Customer classification. Customers of the Group's companies must be segmented and classified by risk as an element that allows the bank to design preventive and control measures that mitigate risk exposure, so that stricter measures and controls can be applied to customers that exhibit a higher risk level.

The controls and procedures must ensure adequate and continuous monitoring of the business relationship with the aim of adapting the risk level, and thus the measures to be applied, to the customer's risk circumstances at all times.

The risk level assessment will be documented in the companies of the CaixaBank Group based on their activity and operations. To determine this classification, various factors will be taken into account depending on the risk exposure of the company and its customers or suppliers, and will include, at a minimum, an analysis of the following factors:

- Customer characteristics:
  - Activity.
  - Geographic area.
  - Politically Exposed Person.
  - Identity of the beneficial owner.
  - Ownership or control structure.
- Characteristics of products or services:
  - Type of product.
  - Business segment.
  - Relationship channel.
- Characteristics of the operation:
  - Source of the funds.
  - Transactions.

At a minimum, Group companies must use the following customer classification, based on the risk level identified:

Persons who are not acceptable as customers: Business relationships with natural or legal persons in any of the following situations are not allowed:

- Individuals to whom the due diligence measures outlined in this policy could not be applied during their onboarding process.
- Persons included in national or international sanctions lists and those who cannot be accepted as customers in compliance with the Sanctions programmes defined in this Policy and in the applicable legal regulations.
- Individuals with businesses whose nature makes it impossible to verify the legitimacy of their operations or the origin of their funds.
- Individuals who refuse to provide documentation that would allow for the owners or real beneficiaries to be fully identified, or who, having provided it, do not agree to let the Bank keep a digital copy of said documentation.
- Individuals who provide documents that are manifestly false, or which cast serious doubts as to their authenticity, legitimacy, lack of tampering, or who do not provide sufficient guarantees.
- Individuals who refuse to provide information or documentation required to justify the declared activities or the origin of their funds, or the purpose and nature of the commercial relationship with the Bank.
- Legal persons or instruments whose ownership structure or beneficial ownership cannot be determined, or companies whose real owner cannot be determined.
- Shell banks and financial institutions that operate with this type of bank.
- Individuals or entities whose activity involves the issuance or brokerage of "cryptocurrencies" or "cryptoassets" in general.
- Individuals or companies that intend to carry out operations corresponding to financial activities, gambling, betting, payment institutions, currency exchange or other activities without having the requisite official authorisation or other legal requirements.
- Any other category not covered by the above that merits rejection in view of the provisions of a legal standard or an internal company policy.

- Natural or legal persons who were Group customers at some point, and who stopped being customers as a result of this policy.

Individuals with a higher-than-average risk: their acceptance as customers shall in any case be contingent upon the application of enhanced diligence measures and will require centralised approval. The following persons or entities will be included in this category:

- Politically exposed nationals and foreigners.
- National and foreign legal persons whose beneficial owners are politically exposed persons (PEP), whether national or foreign.
- Individuals who have their residence in a high-risk jurisdiction.
- Individuals who are nationals of a high-risk jurisdiction and who, due to the presence of a factor considered in the risk matrix, are deemed to have a higher-than-average risk.
- Legal persons that are domiciled or incorporated in a high-risk jurisdiction, or that, having been incorporated or being based in a country other than those considered to be high-risk jurisdictions, are owned or controlled by a person/entity that is a national or resident of a high-risk jurisdiction.
- Private banking customers.
- Correspondent banking relationships.
- Customers related to the production, commercialisation, distribution and sale of arms and other elements of a military nature.
- Electronic money institutions and payment institutions when they engage in money transfer and/or foreign currency exchange activities
- Casinos, recreational gaming companies and other companies linked to gambling that have the corresponding official authorisation or other legally enforceable requirements, as well as any other risk sector where required by its specific procedures.
- Companies with bearer securities, once their ownership or control structure has been determined.
- Any natural or legal person whose characteristics or operations lead the AML/CFT Prevention Unit (UPBC) to conclude that it would be advisable to submit their acceptance as a customer or risk classification for its own consideration.

All other persons or entities will be subject to normal or simplified due diligence measures as established in the applicable laws or internal rules and procedures.

Formal identification of customers. The rules and procedures that implement these Principles must guarantee that the Group companies properly identify all their customers in accordance with the applicable laws for each jurisdiction, which will include, in any case, verifying their identity by means of valid documents.

Under no circumstances will business relationships be maintained with individuals who cannot be identified. Moreover, the contracting of anonymous, encrypted, or fictitious products or services is strictly prohibited.

Before a business relationship is established or a transaction is executed, the real holder must be identified. This obligation will imply that if there are any indications or certainty that customers are not acting on their own behalf, accurate information must be collected in order to determine the identity of the persons on whose behalf they are acting, as well as sufficient documentation to verify their authority.

Knowledge of the customer's activity and assets. Before a business relationship is established, the Group companies must, at a minimum, obtain information on the customer's professional or business activity and the source of their funds or assets.

Depending on the risk level assigned to the customer, additional measures may be adopted consisting of verifying, using reliable external sources, the information provided by the customer, especially in relation to their professional or business activity, the source of their funds or assets, and any other relevant information in accordance with internal rules and procedures.

4.3 Detection, control and examination of operations

Group companies must have the means to detect, control and examine transactions. These measures will be applied based on the risk and will, in any case, include the three basic scenarios for detecting operations:

a. Internal communication of suspicions by Group employees.

b. Detection of possible suspicious transactions through established alert systems (for each Group company and/or centralised).

c. Communications from supervisory bodies or police or judicial authorities.

If suspicious transactions are identified, a detailed and comprehensive analysis will be conducted aimed at determining the effective existence of indications of money laundering and terrorist financing. The methodology for conducting this analysis must be contained in a specific procedure called the Special Examination Procedure. This analysis will be centralised in the same unit for all Group companies operating in the same jurisdiction.

The monitoring will be automated and will review activity based on patterns identified by the law and best practices.

4.4 Reporting suspicious transactions

Group companies will proactively communicate to the supervisory and/or Financial Intelligence bodies any fact or transaction, even mere attempts, that the special examination has determined shows signs or certainty of being related to money laundering or terrorist financing.

In particular, transactions that lack any ostensible connection with the nature, volume of activity or operational background of the customer will be reported to supervisory bodies.

The reporting decision will be taken centrally in each jurisdiction by the persons or bodies designated for this purpose, and the report shall be made to the competent authorities by the authorised representative.

The report made shall, in any case, include information on the decision taken regarding whether or not to continue the business relationship, as well as the justification of this decision.

Without prejudice to reporting the suspicious transaction, the entity shall immediately adopt additional risk management and mitigation measures that must take into account the risk of disclosure.

Group employees must abstain from executing any transaction for which there is an indication or certainty that it is related to money laundering or terrorist financing.

Employees, executives, or agents of the Group will not disclose to the customer or third parties that information has been provided to internal control bodies or the supervisory authority, or that a transaction is being analysed or may be analysed for possible relation to money laundering or terrorist financing.

4.5 Screening sanctions lists and reporting matches

To comply with the restrictions imposed by sanctions programmes, Group companies must:

- Identify and monitor the sanctions programmes established by the United Nations (UN), the European Union (EU), OFAC and local programmes that are applicable in the jurisdictions in which the Group's companies operate.

- Assess the risks associated with the activities related to the sanctions programmes to determine the risks of participating or intervening in activities restricted or prohibited by sanctions.

- Refrain from executing or participating in operations or transactions with sanctioned persons.

- Comply with the prohibitions and restrictions on the execution of transactions, payments or business relations, and refrain from executing them when they are in violation of sanctions programmes.

- Block assets and funds when required by sanctions programmes, and report this situation to the authorities that manage said programmes.

- Implement internal control procedures and prevention mechanisms, to include automated screening procedures and tools, in order to allow adequate compliance with the obligations of the Group's companies.

4.6 Document storage

The companies of the CaixaBank Group will establish document storage policies that comply with the legal requirements applicable in each jurisdiction, with the minimum storage period being that specified by the applicable laws, and never less than 10 years.

The documentation to be stored in accordance with the prevention laws includes at least the following aspects:

- In particular, the following documentation must be kept so that it may be used in any investigation or analysis regarding possible cases of prevention by supervisors, or any other competent bodies:
- Copies of the documents required for the application of due diligence measures, including, in particular, copies of valid identification documents, customer statements, and the documentation and information provided by the customer or obtained from independent reliable sources.
- The original or copy, with evidentiary value, of the documents or records that sufficiently prove operations, the intervening parties thereof, and the business relationships.

- All documentation that formalises compliance with internal reporting and control obligations:
  - Communications to supervisory bodies.
  - Notification of the appointment of representatives to Financial Intelligence authorities.
  - Special examination files.
  - Reports of suspicious transactions sent to supervisory bodies and related documentation.
  - Reporting requirements and tracking requests received from supervisory bodies.
  - Annual reports of the external expert examination and related documents.
  - Minutes of meetings of internal control bodies, and storing as well the minutes and documents of other bodies with regard to aspects that have an impact on prevention.

4.7 Training

Raising awareness of the risks associated with these crimes is a key element in the fight against money laundering and terrorism.

CaixaBank Group companies must define, maintain and apply training programmes for their employees to ensure an adequate level of awareness among all personnel, as required by law, and they will establish policies that guarantee mandatory periodic training in anti-money laundering, terrorist financing and sanctions for all their personnel (including senior management and governing bodies) that is appropriate to the level of risk exposure of their activity in the company.

The AML/CFT training and sanctions programmes of all CaixaBank Group companies must be validated by CaixaBank's Regulatory Compliance unit, which is a specialised unit of the Group, once these have been validated by the company departments responsible for training and compliance. Training records must be stored that document the content of the training and the employees who received and completed it.

4.8 Consolidated risk management

CaixaBank believes that the best way to combat the risks associated with these Principles is through a consolidated approach and the uniform and aggregated processing of the information related to risk management at the Group level, regardless of the jurisdiction in which the companies that comprise it operate.

The principle of aggregated or consolidated management is thus cemented as a fundamental pillar of the prevention model, and it allows the efforts of all Group companies to be coordinated, and risks to be assessed and managed in an aggregated way.

As a result, all the companies that comprise the Group will keep CaixaBank promptly informed of high-risk relationships, data on sensitive activities and their associated risks, quickly responding

to any request for information that CaixaBank may make to manage the regulatory and reputational risk related to money laundering, terrorist financing and sanctions.

In any case, these obligations are understood to be without prejudice to strict compliance with the applicable regulations, particularly those on data protection and privacy. CaixaBank and the Group companies will take the necessary measures to preserve the confidentiality and privacy of any data exchanged between them.