General principles of the Corporate Policy on the Prevention of Money Laundering and on International financial sanctions and countermeasures.

29 June 2023

Contents

1. Introduction

1.1 Background

CaixaBank, S.A. (hereinafter "CaixaBank"), as the parent company of the companies that constitute its group (hereinafter, "Group" or "CaixaBank Group", indistinctly) is firmly committed to anti-money laundering and counter terrorism financing (hereinafter AML/CTF), and to complying with the programmes of international financial sanctions and countermeasures (hereinafter "Sanctions") by actively promoting the implementation of the highest applicable international standards.

Financial crime is a universal, global phenomenon which materializes taking advantage of the disappearance of commercial barriers and the globalisation of the economy. Combating this phenomenon requires and demands a coordinated response by the international community in general and the financial sector in particular, to avoid being inadvertently and involuntarily utilised for unlawful purposes.

1.2 Concept of the risk of Money Laundering, Terrorism Financing and Sanctions

The following definitions are used for the purposes of interpretation and application of these Principles:

Money laundering

- The conversion or transfer of property, knowing that such property is derived from a criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such activity to evade the legal consequences of his or her actions.

- The concealment or disguise of the true nature, source, location, disposition, movement, beneficial ownership of property or rights, knowing that such property is derived from criminal activity or involvement in criminal activity.

- The acquisition, possession or use of property, knowing, at the time of receipt, that such property is derived from criminal activity or from an act of participation in criminal activity.

- Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the actions mentioned in the foregoing points.

Property deriving from criminal activity means assets of every kind whose acquisition or possession originates from a crime, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets, and the amount defrauded in the case of tax fraud.

Money laundering shall be regarded as such even where the activities which generated the property were carried out in the territory of another Member State or in that of a third country.

Finally, please note that the following stages are usually distinguished in the money laundering process:

1. **Placement or concealment**: introducing cash from criminal activities into financial circuits or exchanging it for other kinds of assets.

2. **Layering**: carrying out transfers or movements among different products or services in one or more jurisdictions for the purpose of breaking up, accumulating, concealing, transferring the amounts and depositing them in jurisdictions that are less stringent in their investigations into the origins of large fortunes or in accounts where the origin of the money has an appearance of legitimacy, or carrying out any other transactions which prevent the true origins from being traced.

3. **Integration**: investing money into the financial system with an appearance of legitimacy.

Entities and companies of the CaixaBank Group may be used during any phase of the process described, mainly during the "placement" phase. Hence, necessary internal control measures must be taken to manage this risk.

Financing of terrorism
The provision, depositing, distribution or collection of funds or property, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, to carry out any of the terrorist offences punishable under the applicable criminal laws and regulations. .

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

Programmes of sanctions and international financial countermeasures
Political, diplomatic or economic instruments used by countries and international or supranational bodies with the purpose of implementing restrictive measures to prevent infringements of international law, of human rights or of civil rights and liberties.

1.3 Purpose

The purpose of this document is to set out the basic principles that regulate the risk of money laundering and terrorism financing ("ML/TF") and Sanctions.

The intention of these General Principles of the Corporate Policy on AML/CTF and Sanctions (the “Policy”) is to establish a framework of compliance in the Group that every company must implement in the development of its activities, its business and relationships, both national and international, in order to prevent money laundering and terrorism financing, as well as to comply with the various applicable international financial sanctions and countermeasures programmes.

2. Scope

These Principles are corporate principles. As a result, these guidelines are applicable to all the companies of the CaixaBank Group that engage in any of the activities included within its scope. The governance bodies of these companies will take the necessary decisions in order to integrate the provisions of these Principles. They will apply the principle of proportionality to adapt the governance framework to the idiosyncrasy of their structure of governance bodies, committees, and departments, as well as their principles of action, methodologies, and processes to the content of this document.

This integration may involve, among other decisions, the approval of an own policy by the relevant company. Such approval will be necessary in those companies that need to adapt the content of these Principles to their own specific characteristics, in terms of subject matter, of jurisdiction or of the risk relevance in the company. In this case, the Compliance function at CaixaBank (*Compliance* Office), given its corporate nature, will seek to align these policies with the corporate policy and the consistency within the entire CaixaBank Group.

Moreover, in those cases in which the company's risk control and management activities are performed directly by CaixaBank, either due to the materiality of the risk in the company or for reasons of efficiency or because the company has externalised the operational management of that risk to CaixaBank, the governing bodies of the relevant companies will acknowledge the existence of this corporate Policy and its applicability to each of them.

3. Regulatory framework Applicable standards and regulations

These Principles shall be governed by the pertinent legislation in force at all times and any legislation amending or replacing it in the future. Specifically, at the date of preparation, the pertinent regulations applicable to the parent entity of the Group are as follows:

- Act 10/2010 of 28 April on the prevention of money laundering and financing of terrorism.
- Royal Decree 304/2014 of 5 May, which approves Act 10/2010 of 28 April, on preventing money laundering and terrorism financing.
- Law 12/2003, of 21 May, on blocking the financing of terrorism.
- Regulations of the European Union on anti-money laundering.
- Regulations of the European Union on international financial sanctions.
- Standards of international organisations, mainly represented by the Recommendations of the Financial Action Task Force (FATF).

With regard to companies or, as the case may be, branches subject to foreign jurisdictions or additional sectoral regulations, any policies and procedures developed by such entities shall take into account, in addition to their own regulations, the obligations at consolidated level as contained in applicable law and regulations, provided that they do not contradict the specific requirements of the corresponding jurisdiction or sectoral regulations.

Finally, the frameworks, standards, guidelines and procedures required for the correct implementation and execution of and compliance with these Principles will be implemented by each of the Group's subsidiaries and branches.

4. Management framework for AML/CTF and Sanctions

The main principles and standards of the AML/CFT prevention framework regulated by these Principles are:

1. Risk assessment
2. Due diligence
3. Detection, control and examination of transactions
4. Reporting of suspect transactions
5. Control over sanctions lists and disclosure of incidents
6. Retention of documentation
7. Training
8. Consolidated risk management

4.1 Risk assessment

The exposure of Group companies to the risks of money laundering, the financing of terrorism and sanctions is directly related to the type of business or activity, the products and services provided, the marketing channels, the type and characteristics of their customers and/or the jurisdictions in which they operate.

In order to maintain a proper control and prevention framework with a risk-based approach, Group companies must be categorised in accordance with their level of risk, thus ensuring a higher level of supervision of companies, segments, channels, jurisdictions or products carrying higher levels of risk are subject .

4.2 Due diligence

The customer acceptance policy and the due diligence measures shall not, in any case, involve a violation of rights in the jurisdictions where the Group company carried out its activities.

The customer acceptance policy is a dynamic process, following a compliance framework at Group level that may vary depending on the degree of risk exposure to certain segments or activities at any given time. The customer acceptance policy must comply with international standards and the Know Your Customer principle(known under the “KYC” acronym), focusing on the need to ensure an adequate ongoing knowledge of the customer and its activities.

The Know Your Customer principle and due diligence policies shall always be applied with a risk-based approach and must ensure that the measures applied are proportionate to the underlying risk of money laundering, terrorist financing or Sanctions.

Classification of customers. The customer of the Group's companies must be segmented and classified based on their risk so that preventive and control measures can be designed that mitigate risk exposure. Thus, stricter measures and controls will be applied to those customers who exhibit a higher level of risk.

Controls and procedures must ensure a proper and ongoing monitoring of the business relationship in order to adapt the level of risk, and therefore the measures to be applied, to the circumstances of the customer's risk at any time.

The assessment of the risk level shall be documented at CaixaBank Group companies on the basis of their activities and operations. When classifying customers, factors relating to the company's risk exposure and the nature of its customers or suppliers shall be taken into account, including an analysis of the following minimum factors:

- Customer characteristics:
  - Activity.
  - Geographic area.

- Politically Exposed Person (PEP).
- 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:
  - Origin of funds.
  - Transactions

As a minimum standard, the Group companies shall use the following customer classification, based on the level of risk identified:

Persons who cannot be approved: Business relationships with individuals or legal entities in any of the following situations cannot be permitted:

- Persons who, during the admission process, could not be subjected to the due diligence measures set out in this policy.
- Persons included in national or international lists of Sanctions and those that cannot be approved as customers pursuant to the programmes of Sanctions defined in this Policy and in the legal provisions applicable in this regard.
- Persons operating businesses the nature of which makes it impossible to verify the legitimacy of their transactions or the origin of their funds.
- Persons refusing to supply documentation to allow for the full formal identification of the beneficial owner or who, having supplied such documentation, refuse to allow the Bank to retain a digitalised copy of it.
- Persons supplying documents that are manifestly false or raise serious doubts as to their legality, legitimacy and non-manipulation, or who do not provide sufficient guarantees.
- Persons refusing to provide the information or documentation needed to verify the activities declared by them or the origin of their funds, or to verify the purpose and nature of their commercial relationship with the Bank.
- Persons and legal instruments in relation to which the ownership or control structure cannot be determined, or companies the real owner of which cannot be ascertained.
- Shell banks and financial institutions operating with this type of banks.
- Persons or entities whose activity consists of issuance or intermediation of cryptocurrencies or crypto-assets, in general.
- Persons or entities attempting to carry out transactions in relation to financial activities, gambling, betting, payment institutions, currency exchange or other activities without official permits or other mandatory requisites.
- Any other category not mentioned above and who must be rejected pursuant to a law or to an internal company policy.
- Individuals or legal entities which were Group customers at some point and ceased to be customers pursuant to this policy.

Persons with a higher-than-average risk: acceptance of these persons as customers is in any event subject to the application of enhanced due diligence measures, and shall require centralised approval. The following persons or entities shall be included in this category:

- Foreign and national politically exposed persons.
- Foreign and national legal persons the beneficial owner of which is a foreign or national politically exposed person (PEP).
- Individuals or legal entities resident in or native to a high-risk jurisdiction, and those that, although not actually in this situation, are controlled by individuals or entities in high-risk jurisdictions.
- Private banking customers.
- Correspondent relationships.
- Customers related to the production, commercialisation, distribution and sale of arms and other elements of a military nature.
- Electronic money and payment institutions when they carry out money transfer services and/or foreign currency exchange.
- Casinos, companies operating recreational gaming and other companies with links to gambling that possess the corresponding official permit or meet any other applicable legal requirements, and any other risk sector when the relevant procedures so require.
- Companies with bearer securities, when their ownership or control structure has been ascertained.
- Any natural or legal person whose characteristics or operations lead the AMLU to conclude that it should be submitted to it for approval prior to its acceptance as a customer.

Everyone else, and entities, shall be subject to normal or simplified diligence measures as specified in the applicable law or in internal rules or procedures.

Formal identification of customers. The standards and procedures that implement these Principles must guarantee that Group's companies properly identify all customers in accordance with the applicable law and jurisdiction, which shall include, in any case, the verification of their identity through valid and unexpired documents.

Under no circumstances shall business relationships be continued with persons who have not been identified. Contractinganonymous, encrypted or fictitious products or services will be forbidden.

Prior to the establishment of business relationships or transactions, the beneficial owner involved must be identified. This obligation implies that, in the event of indications or certainty that customers are not acting on their own behalf, precise information must be compiled to ascertain the identity of the parties on behalf of which they are acting. There must also be sufficient documentation to evidence the powers of attorney that are being used.

Knowledge of the customer's activity and assets. Before a business relationship is established by a Group company, it shall gather, as a minimum standard, information on the professional or business activity of the customer and the source of their funds or assets.

Depending on the level of risk assigned to customers, further measures may be applied, consisting of verification by means of documents and reliable external sources of the information supplied by customers, especially in connection with their professional or business activity, the origin of the funds or assets and any other relevant information in accordance with internal procedures and regulations.

4.3 Detection, control and examination of transactions

Group companies must have the resources for detecting, controlling and examining transactions. These resources shall be applied based on risk, and in any case shall entail the three basic premises of detection of transactions:

a. Internal reporting of indications by Group employees.

b. Detection of possible suspicious transactions through the transaction monitoring systems (at each Group company and/or on a centralised basis).

c. Notifications by supervisory bodies or police or court authorities.

The detection of suspicious transactions involves a detailed and comprehensive analysis aimed at determining the effective existence of signs of money laundering and the financing of terrorism. The methodology for performing this analysis must be set out in a specific procedure known as the Special examination procedure. This analysis shall in any case be centralised at a unit common to all Group companies operating in the same jurisdiction.

The monitoring system shall be automated, reviewing activities on the basis of the standards prescribed by the law from time to time and in accordance with best practices.

4.4 Reporting of suspect transactions

Group companies shall voluntarily report to the supervisory bodies and/or Financial Intelligence units any event or transaction or any attempted event or transaction which, following the special examination, determines that the transaction shows indications or certainty of links to money laundering or the financing of terrorism.

Specifically, supervisory bodies shall be notified of any transactions showing any ostensible inconsistencies in relation to the nature or volume of activity of past operations of customers.

The decision to report shall be taken in a centralised fashion in each jurisdiction by the persons or bodies designated to this end, and the report shall be made by the official representative with the competent authorities. The report shall in any case contain information on the decision taken with respect to continuation of the business relationship, and the justification for this decision.

Notwithstanding the report through indications, the bank shall immediately take further measures to manage and mitigate risk, and these must take account of the risk of disclosure.

Group employees must refrain from carrying out any transactions with respect to which there are indications or certainty of links to money laundering or the financing of terrorism.

Group employees, management or agents shall not disclose to the customer or to third parties that information has been reported to internal control bodies or to the supervisory body, or that transactions are being examined or may be examined to ascertain if they involve money laundering or the financing of terrorism.

4.5 Control of lists of Sanctions and notification of detections

To ensure compliance with the restrictions imposed by programmes of Sanctions, Group companies must:

- Identify and follow the Sanctions' programmes established by the United Nations (UN), the European Union (EU), OFAC and any applicable local programmes in the jurisdictions in which the Group companies operate.

- Assess the risks associated with the activities related to the Sanctions' Programmes in order to determine the risks of taking part or being involved in activities that are restricted or forbidden by Sanctions.

- Abstain from agreeing to or participating in operations or transactions with sanctioned individuals.

- Enforce prohibitions and restrictions when executing transactions, payments or business relationships, and abstain from executing them when they entail violating a Sanctions programme.

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

- Implement internal control procedures and prevention mechanisms for proper compliance with the obligations of Group companies, which shall include procedures and tools for automated filtering (screening).

4.6 Retention of documentation

CaixaBank Group companies shall establish documentation retention policies that meet the legal requirements applicable in each jurisdiction. The minimum retention period shall be as determined by pertinent legislation at any given time, and shall never be less than 10 years.

The documentation that must be kept in accordance with applicable AML/CTF law includes the following as a minimum:

- Specifically, it shall store information for use by supervisors or by any other competent authority in any investigation or analysis involving potential prevention cases.
- Copies of documents which are mandatory for the purposes of due diligence measures, specifically including copies of documents substantiating identification, statements by the customer, documentation and information supplied by the customer or obtained from reliable independent sources.
- Originals or probatory documents or registers properly accrediting the transactions, the parties involved in the transactions and business relationships.
- Any documentation formalising compliance with reporting obligations and internal control obligations:
    - Communications to supervisory bodies.
    - Notification of the appointment of representatives for Financial Intelligence authorities.
    - Special examination files.
    - Reports of suspicious transactions sent to supervisory bodies and documentation in connection with these reports.
    - Information requirements and tracking requests received from supervisory bodies.
    - Annual reports on examinations by external experts and related documents.
    - Minutes of the meetings of internal control bodies, with a record also kept of the minutes and documents of other bodies with respect to aspects affecting prevention.

4.7 Training

Creating awareness of the risks associated with these crimes is a key feature of the fight against money laundering and the financing of terrorism.

CaixaBank Group companies must define, maintain and apply employee training programmes to ensure a proper level of awareness among all staff members, as required by law, and must establish policies to guarantee mandatory training in anti-money laundering, counter terrorist financing and Sanctions for all staff members (including senior management and governance bodies) on a regular basis in accordance with the level of risk their activities carry within the company.

CaixaBank's Regulatory Compliance unit shall validate the AML/CTF and Sanctions training programmes in place at each CaixaBank Group company once those programmes have been validated by the Group company's training and compliance departments. A record shall be kept of all training delivered, including subject matter and content and the names of the employees who successfully completed the training.

4.8 Consolidated risk management

CaixaBank believes that the best way to combat the risks associated with these Principles is to manage said risks in a uniform manner, and to manage all the information related to the handling of these risks at a Group level, regardless of the jurisdiction in which the Group companies operate.

The principle of aggregate or consolidated management is thus one of the pillars of the prevention model, and coordinates the efforts of all Group companies uniformly, and also assesses and manages risk in an aggregate fashion.

Thus, all companies that are part of the Group shall keep CaixaBank regularly informed of high-risk relationships, data on sensitive activities and their associated risks, responding rapidly to any information requests that may be issued by CaixaBank in its management of regulatory and reputational risk in connection with money laundering, the financing of terrorism and Sanctions.

In any case, these obligations are understood without prejudice to strict compliance with the regulations applicable, most particularly regulations concerning data protection and privacy. CaixaBank and all Group companies shall take the necessary steps to protect and uphold the confidentiality and privacy of all data thus reported between Group companies.