CaixaBank Group's General Principles of the Corporate Policy on the Prevention of Money Laundering and Terrorist Financing and International Sanctions and Financial Countermeasures

[September 2021]

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 preventing money laundering and the financing of terrorist activities (hereinafter ML/TF), and to complying with the Programmes of International Financial Sanctions and Countermeasures (hereinafter "Sanctions") by actively promoting the application of the highest international standards in the field.

Financial crime is a universal, global phenomenon which homes in on the disappearance of commercial barriers and the globalisation of the economy to materialise. Combating this phenomenon requires and demands a coordinated response by the international community in general and the finance sector in particular, to prevent themselves from 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 prevention

- The conversion or transfer of goods, knowing that these goods stem from a criminal activity or from taking part in a criminal enterprise, with the intention of concealing or hiding the illicit origin of the goods, or of helping those involved to avoid the legal consequences of their actions.

- Concealing or disguising the real nature, origins, location, provision, movement or ownership of assets or entitlements to assets, in the knowledge that these assets originate from a criminal activity or from participation in a criminal activity.

- Acquiring, possessing or using assets in the knowledge, when they are received, that they originate from a criminal activity or from participation in a criminal activity.

- Participation in any of the activities stipulated in the preceding paragraphs, association to perpetrate such acts, attempting to perpetrate them and assisting, instigating or advising someone to perpetrate them or assist in perpetrating them.

Assets that originate from a criminal activity shall be understood as any assets the acquisition or possession of which originates from a crime, material or non-material assets, real estate or movables, tangible or intangible, and any legal documents or instruments irrespective of their format, including electronic or digital formats, accrediting ownership of such assets or entitlement to them, including the amount of tax evasion in the event of fiscal crimes.

Money laundering shall be considered to exist even if the activities which generated the assets were carried out on the soil of another State.

Finally, it should be noted that the following phases are usually distinguished in the money laundering process:

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

2. **Accumulation**: Carrying out transfers or movements among different products or services in a jurisdiction or jurisdictions for the purposes 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 a legal semblance, or carrying out any other transactions which prevent the true origins from being traced.

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

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

Financing of terrorism
Supplying, depositing, distributing or collecting funds or assets, by any means, directly or indirectly, with the intention of using them or in the knowledge that they shall be used, totally or partially, to perpetrate any of the terrorist crimes stipulated in the criminal regulations applicable.

The financing of terrorism shall be considered to exist even if the funds or assets were supplied or collected on the soil of another State.

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

1.3Aim

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 ML/TF and Sanctions (the "Policy") is to establish a framework of compliance at Group level that every company has to observe over the course of its activities, business and relationships, both nationally and abroad, to prevent money laundering and terrorism financing, as well as to comply with the various international financial sanctions and countermeasures programmes that may apply.

2. Scope

These Principles are corporate in nature. As a result, the guidelines defined 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 make the decisions necessary 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 entail, among others decisions, the approval of a single internal policy by the company. This approval will be necessary in those companies that need to adapt the content of these Principles to their own specific situation, whether in terms of the subject matter, the jurisdiction or the significance of the risk in the company. In this case, the compliance function in CaixaBank, given its corporate nature, will seek to align these policies with the corporate policy in a way that is consistent throughout the CaixaBank Group.

Moreover, in those cases in which the company's risk control and management activities are done 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 to CaixaBank the operational management of that risk, the governing bodies of the affected companies will acknowledge the existence of this corporate Policy and of its application to said companies.

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.

In the case of companies subject to foreign jurisdictions or supplementary industry regulations, the policies and procedures that these companies develop shall take into account not only their own regulations, but the consolidated obligations contained in the aforementioned law, as long as they do not contradict the specific requirements in the relevant jurisdiction or industry regulation.

Lastly, each Group company shall develop the necessary rules, guidelines or procedures to ensure the effective implementation, execution, and observance of these Principles.

4. Management framework for ML/TF and Sanctions

The main principles and standards constituting the prevention framework regulated by these Principles are as follows:

1. Risk Assessment
2. Due diligence
3. Detection, control and examination of transactions
4. Reporting of suspect transactions
5. Control of lists of Sanctions and notification of detections
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 sold, the services provided, marketing channels, the typology and characteristics of customers and/or any jurisdictions in which they may 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 to guarantee the application of greater supervision of companies, segments, channels, jurisdictions or products with higher levels of risk.

4.2 Due diligence

The customer approval policy and the due diligence measures shall not, in any case, entail a violation of rights in the jurisdictions where the Group company performs its activities.

Customer approval policy is a dynamic process, and establishes a compliance framework at Group level which may vary in accordance with the levels of risk in certain segments or activities, depending on exposure to risk at any given time. The approval policy shall comply with international standards and with the "Know Your Customer" principle, with a special focus on guaranteeing that proper knowledge of the customer and their activities is available at all times.

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

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

Controls and procedures must ensure proper continuous 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.

Appraisals of the level of risk 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.

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

Persons who cannot be approved: Business relationships with natural or legal persons included in the national or international sanctions lists or those to whom it has not been possible to apply the due diligence measures established in Law 10/2010, as well as any other case provided for by a legal regulation or by the bank's internal policy, shall not be accepted.

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.

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 documents.

Under no circumstances shall business relationships be continued with persons who have not been identified, and products or services may not be contracted anonymously, through encryption or in a fictitious format.

Prior to the establishment of business relationships or transactions, the real party 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 accredit authorisation for their actions.

Knowledge of the customer's activity and assets. Before a business relationship is established by a Group company, it shall gather, at a minimum, 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 scenarios of detection of transactions:

a. Internal reporting of indications by Group employees.

b. Detection of potential suspect transactions through the alert systems established (systems at each Group company and/or centralised systems).

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

The detection of suspect transactions entails 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, and shall conduct a review of activities on the basis of the standards identified at any given time by the law and best practices.

4.4 Reporting of suspect transactions

Group companies shall voluntarily report to the supervisory bodies and/or Financial Intelligence 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 grounds for this decision.

Notwithstanding the report through indications, the bank shall immediately take further measures to manage and mitigate risk, and this 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 conservation policies which meet the legal requirements applicable in each jurisdiction. The minimum conservation period shall be as determined by pertinent legislation at any given time, and shall never be less than 10 years.

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.

The ML/TF and Sanctions training programmes of every company in the CaixaBank Group shall be validated by the Regulatory Compliance unit at CaixaBank once said programmes have been validated by the company's training and compliance departments. A record shall be kept of the training given, its content, and the employees who received and 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 mainstays 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 making up 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.