



General principles of CaixaBank Group Corporate Policy for Anti-Money Laundering and Counter Terrorist Financing and for management of Sanctions and International Financial Countermeasures

[July 2020]

Contents

I. Basis and objectives	3
II. Concepts	3
III. Scope of application	4
IV. Prevention framework	4
1. Risk Assessment	5
2. Due Diligence	5
3. Detection, control and examination of transactions	6
4. Reporting of suspect transactions	7
5. Control of lists of Sanctions and notification of detections	7
6. Retention of documentation	7
7. Training	8
8. Roles and responsibilities	8
V. Governance	8
VI. Approval and publication	9

I. *Basis and objectives*

CaixaBank, S.A. (hereinafter "CaixaBank"), as the parent of the companies which make up its Group (hereinafter referred to together as either the "Group" or the "CaixaBank Group") is firmly committed to the prevention of money laundering, to the prevention of the financing of terrorist activities and to compliance with Programs of Sanctions and International Financial Countermeasures (hereinafter "Sanctions"), and proactively applies the most stringent international standards in this regard.

Financial crime is a universal and global phenomenon which homes in on the disappearance of commercial barriers and the globalization of the economy to materialize. 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 utilized for unlawful purposes.

The purpose of these General Principles of Corporate Policy for Anti-Money Laundering and Counter Terrorist Financing and for management of Sanctions and International Financial Countermeasures (hereinafter the "Principles") is to (i) establish a **framework of compliance** at Group level which must be applied by all companies in the exercise of their activities, areas of business and relations both at home and abroad to prevent money laundering and the financing of terrorism and to comply with the various programs of sanctions and international financial countermeasures applicable; (ii) define roles and responsibilities in this area; (iii) provide a basis for the definition and application of policies and procedures at Group subsidiaries; and (iv) establish the governance framework.

The application of the measures set out in these Principles must guarantee mandatory compliance with the regulations applicable in all jurisdictions where the CaixaBank Group exists and operates.

II. *Concepts*

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

Money laundering:

- Converting or transferring assets, in the knowledge that these assets originate from a criminal activity or from participation in a criminal activity, for the purposes of concealing or disguising the unlawful origin of the assets or assisting any parties involved to elude 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.

Programs 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.

III. *Scope of application*

The Principles are applicable to all CaixaBank Group companies that are obliged to adhere to it by anti-money laundering regulations or programs of Sanctions. The Policy must be adopted in all jurisdictions where CaixaBank and its subsidiaries conduct their activity, relations or business.

IV. *Prevention framework*

The main principles and standards constituting the prevention framework 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. Roles and responsibilities
9. Consolidated risk management

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 categorized 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.

2. Due Diligence

The policy for approval of customers and due diligence measures may not under any circumstances entail any infringement of rights in jurisdictions in which the Group Company conducts its business.

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 must meet international standards and the "KYC" principle, Know Your Customer, with a particular focus on guaranteeing proper knowledge of customers and their activities 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.

- 2.1.1. Classification of customers. Customers of Group Companies must be segmented and classified in accordance with risk as a feature to devise prevention and control measures to mitigate exposure to risk, to enable stricter measures and controls to be applied to customers showing greater 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. For the purposes of determining this classification, at least the factors relating to the company's exposure to risk and its customers or suppliers shall be taken into account.

Group Companies must at least use the following customer classification, depending on the level of risk identified:

- 2.1.1.1 **Persons that cannot be admitted:** Business relationships with individuals or legal entities that are included on national or international lists of Sanctions or those that could

not be subjected to the due diligence measures set out in 10/2010 law, as well as any other case foreseen by legal regulations or by the Company's internal policy.

2.1.1.2 **Persons of above-average risk:** acceptance of these persons as customers is in any event subject to the application of enhanced due diligence measures, and shall require centralized approval.

2.1.1.3. Other persons or entities shall be subject to **normal or simplified due diligence measures** as established in the regulations applicable or in internal regulations and procedures.

- 2.1.2. Formal identification of customers: any regulations and procedures must ensure that Group Companies properly identify all their customers in accordance with the legislation applicable at any given time and in each jurisdiction, which in any case shall include verification of identities by means of valid and current 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 beneficial owner must be identified.

- 2.1.3. Knowledge of the customer's activity and assets: before a business relationship is established, Group companies must at least compile information concerning the customer's professional or business activity and the origin of the 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.

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 centralized 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.

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. 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 centralized 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, managers 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.

5. Control of lists of Sanctions and notification of detections

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

- Identify and follow the programs of Sanctions established by the United Nations (UN), the European Union (EU), the OFAC and any local programs applicable in the jurisdictions in which the Group companies operate;
- Assess the risks associated with activities relating to the Programs of Sanctions for the purposes of determining the risks of participation or involvement in activities restricted or prohibited by the Sanctions;
- Refrain from carrying out or participating in operations or transactions with sanctioned parties;
- Adhere to prohibitions and restrictions in carrying out transactions, making payments or in commercial relations, and refrain from carrying them out when they entail non-compliance with the programs of Sanctions;
- Block access to assets and funds when required to do so by the programs of Sanctions, notifying these circumstances to the authorities administering the programs of Sanctions;
- 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).

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.

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's companies must define, maintain and apply employee training programs to guarantee a proper level of awareness among all staff, as required by law, and shall establish policies to guarantee mandatory training in anti-money laundering, counter terrorist financing and Sanctions for all staff (including senior management and the board of directors) on a regular basis in accordance with exposure to risk in their company activities.

8. Roles and responsibilities

As per regulations, CaixaBank Group companies must have a governance structure and internal organization to meet their obligations concerning identification and anti-money laundering, counter terrorist financing and Sanctions, guaranteeing proper compliance with reporting obligations in each jurisdiction to the competent authorities for each company, and also guaranteeing proper lock-down and freezing of funds or economic resources arising from the application of international sanctions and countermeasures.

Responsibility for applying processes to identify customers shall mainly lie with those who are in direct contact and conduct relations directly with customers and are directly involved in the initial establishment of relations with customers, applying the policies concerned (first line of defense) at all times.

By way of an independent second line of defense, the main activities of the Anti-Money Laundering and Counter Terrorist Financing function, among others, shall be as follows:

- Definition and implementation of prevention policies, regulations and procedures.
- Supervision of the application of and compliance with prevention policies, regulations and procedures, using a risk-based approach.
- Definition of a compliance program and plan for the purposes of compliance with the regulations applicable.
- Validation and supervision of internal controls to ensure proper knowledge of customers.
- Maintaining fluid contact and communications with supervisory bodies, authorities and regulators.
- Conducting a regular appraisal of risk exposure and proposing corrective and remedial measures to make good any weaknesses or non-compliances.

The Internal Audit function shall carry out regular reviews of the most relevant aspects of the functions involved in the Group prevention model and their adaptation to this Policy and to the other regulations and procedures applicable.

V. Governance

Implementation of the prevention, management, control and decision-making functions addressed in these Principles and their implementing regulations requires a solid governance structure to guarantee the involvement of CaixaBank's decision-making bodies and management and administration units, and close cooperation among Group companies.

To this end:

- The management bodies of each Group company shall be responsible for the following tasks:
 - Undertaking ultimate responsibility for approving and applying these Principles and any regulations implementing same;

-
- Supervising compliance with rules and regulations in this regard;
 - Ensuring the adoption of any corrective, mitigation and remedial measures identified as the consequence of internal control procedures or supervisory activity;
 - Approving the appetite for risk.
- CaixaBank may also determine and define other collegiate bodies or committees with responsibility for this issue at Group level, as non-statutory bodies.

VI. *Approval and publication*

These Principles and any subsequent amendments and updates thereof must be approved by the CaixaBank Board of Directors.

These Principles will be made available at the public corporate site of Caixabank S.A.