

# **AML/CFT – Policy Summary**



**Edition:** March 2024

## **Anti-Money Laundering / Counter Terrorist Financing – Policy Summary**

### **1 INTRODUCTION**

Objective: Maintain high standards with all AML/CTF regulations to avoid Banco Bradesco Europa S.A. (“the Bank”) being used as an intermediary for deposits and transfers of funds derived from criminal activity. It is the Bank’s commitment to comply with Luxembourgish AML laws and regulations to prevent it from becoming an unwitting participant in any illegal activity with the consequent damage to its reputation in the market place.

All members of the staff must maintain an appropriate level of awareness of the Bank’s corporate AML/CTF obligations and of their own personal AML/CTF obligations and of the potential severe penalties imposed by the authorities for non-compliance. Employees with direct or indirect contact with clients must be particularly alert in this regard. All members of the staff must also promptly report any suspicious money laundering or terrorist financing transactions to the Chief Compliance Officer and Money Laundering Reporting Officer.

It is mandatory that proper documentation be requested from new clients prior to the initiation of any relationship. Under the “know your client” principle the relationship between a financial institution and its client is established personally. The opening of business relations implies a judgment on the client, duly supported by information about his activities and purpose of business.

The information obtained by the Bank prior to the establishment of a client relationship should enable the detection of transactions that are not consistent with the clients’ business or professional activities, therefore reducing the risk of the institution being used for money laundering purposes.

### **2 LEGAL BACKGROUND**

The Bank is subject to the Laws and Regulations of Luxembourg, as well as the Regulations and Circulars of the Commission de Surveillance du Secteur Financier (CSSF) which is the competent authority in charge of the financial market in Luxembourg.

In particular:

- Luxembourg law of 12 November 2004 as amended on the fight against ML and TF, transposing directive 2001/97/EC of the European Parliament and Council of 4 December 2001 modifying the directive 91/308/EEC of the Council relating to the prevention of the use of the financial system for ML purposes and modifying certain legislation (herein referred to as the “AML Law”);
- Grand Ducal Regulation of 29 October 2010 enforcing the law of 27 October 2010 implementing the UN Security Council resolutions and EU acts on interdiction and restrictive financial measures against certain persons, groups or entities in the context of the fight against financing of terrorism, as amended;
- CSSF Regulation 12-02 dated 14 December 2012, as amended, on the professional obligations for the fight against ML and the TF.

### 3 OBJECTIVES / PRINCIPLES

The Bank has a zero tolerance for financial crime, including Money Laundering (ML), Terrorist Financing (TF) and Proliferation Financing (PF). This is reflected in the culture and values of the Bank. The following guiding principles underpin the development of policies and procedures in relation to ML, TF and PF and in this respect. The Bank will:

- Undertake and maintain, on an on-going basis, an AML Risk Assessment to identify areas where the Bank may be susceptible to an increased risk of being a conduit of Financial Crime;
- Undertake and maintain, on an on-going basis, an AML Risk Appetite Statement which can be defined as the amount and type of risk that the Bank is prepared to pursue, retain or take. It's a strategic orientation of the direction the Bank wants to take while doing business, and is dynamic and shall adapt to changes in the business and environment (e.g., legal and regulatory, business activities, any other external or internal factors).
- Ensure the compliance of the Bank with the laws, rules and regulations, which address the prevention and the fight against money laundering and terrorist financing;
- Ensure the compliance of the Bank with all internal policies of Money Laundering Prevention, including the establishment of new business relationships and/or opening of new accounts and other related controls;
- Verify clients details prior to the establishment of any relationship and ensure ongoing monitoring of continuing relationships to ensure that the Bank reduces the risk of the business being used to further Financial Crime, by means of the adoption of an effective transaction monitoring system, procedures and internal controls;
- Ensure Client Due Diligence ("CDD") measures are applied on a risk-based approach;
- Ensure Enhanced Due Diligence ("EDD") measures are applied in high risk situations, such as PEP's;
- Only rely on third party verification where it is appropriate to do so;
- Conduct monitoring in respect of any third parties on which we rely to ensure that this reliance remains appropriate on an on-going basis;
- Establish and maintain appropriate record-keeping procedures;
- Make effective use of client information for money laundering prevention;
- Keep full records of all transactions;
- Set up internal reporting procedures for suspicious activities, including the appointment of a Money Laundering Reporting Officer ("MLRO") to process disclosures to the local Financial Intelligence Unit (i.e. Cellule de Renseignement Financier "FIU") or, in the case of foreign branches, to the appropriate local authority;
- Clearly identify and designate the responsibilities and assignments throughout the Bank's structure and operational levels;
- Establish processes and procedures with a view to developing and promoting staff awareness and training programs and train relevant employees in their obligations and in the procedures for recognising and reporting suspicions of money laundering;
- Notify and cooperate with relevant regulatory authorities should the Bank be required to do so; and
- Monitor compliance with these guiding principles;
- Protect the Bank's reputation and image.

## 4 RESPONSIBILITIES

The responsibilities for the observance and compliance with the AML Policy are incumbent upon all members of staff, who count on the commitment of the Bank's Board of Directors. Specifically, these responsibilities are described as follows:

- The Bank's Board of Directors

To establish institutional guidelines in order to ensure compliance with Laws and Regulations, making the AML Policy effective, designating managers and assigning their responsibilities;

- Senior Management

Senior management of the Bank are responsible for the establishment and maintenance of effective anti-money laundering systems and controls. Certain core obligations exist for the Bank's senior management as follows:

- Identifying, assessing, monitoring and managing effectively, the AML and financial crime risks in our businesses
- Ensure that the Bank's systems and controls are comprehensive and proportionate to the nature, scale and complexity of the Banks' business activities.
- Appoint a Nominated Officer to process disclosures
- Appoint a MLRO
- Provide adequate information and resources to be devoted to AML, financial crime and CTF.

- Compliance Officer

The Compliance Officer is responsible, amongst others, for the following:

- Identify and assess the AML/CTF risks associated with the Bank's current and proposed future business activities, including new products and business practices, including new distribution mechanisms, and the use of new or developing technologies related to new or pre-existing products;
- Identify and keep an inventory available to all staff of essential laws and regulations pertinent to the Bank;
- Advise the Bank's Management on the applicable laws, regulation, rules and standards and inform them about any developments in these areas;
- Establish written guidelines to staff and service providers on the appropriate implementation of the laws, regulations, rules and standards through policies and procedures;
- Assess the appropriateness of internal policies, procedures and guidelines;
- Ensure a follow-up of any identified deficiencies, and make recommendations for amendments, where necessary, and supervise the implementation of corrective measures to mitigate the identified deficiencies;
- Monitor compliance with internal policies, procedures and guidelines by performing regular and comprehensive compliance risk assessments and testing; report the results on a regular basis and promptly where deemed necessary to the Bank's Management and to the Board of Directors;
- Train staff with respect to compliance with the applicable laws, rules and standards and act as advisor on compliance queries from staff members;
- Exercise specific legal responsibilities (e.g. reporting suspicious transactions related to money laundering and the fight against terrorism financing).

- Staff Member

Each employee has personal responsibilities in relation to preventing ML, TF and PF. This includes:

- To report any knowledge or suspicion of money laundering to the MLRO as soon as possible;
- To never assist someone known to be, or suspected of being, a money launderer;
- Not to tell a client, or others outside the Bank or indeed other colleagues in the Bank (except on a "need to know" basis), of a money laundering suspicion or that an investigation is in progress ("Tipping Off");
- To keep thorough, comprehensive and up-to-date records on client information and transactions, reporting and training; and
- To maintain an up-to-date knowledge of the AML Policy and related policies and procedures.

## 5 MAIN PROVISIONS

The main provisions guiding the AML Policy are the following:

- Due Diligence measures: The Bank adopts the necessary controls to obtain the full identification and verification of its customers, investors, savers and consumers of products and/or services;
- Enhanced Due Diligence measures: The Bank applies on a risk sensitive basis, enhanced client due diligence measures in addition to the standard client due diligence in situations which by their nature can present an exposition to a higher risk of money laundering or terrorist financing (e.g. PEP's);
- On-going monitoring: The Bank has put in place a CDD periodic review of each client on a risk-based approach. The results of each review should be performed by the relationship officers and their respective teams and documented on the file for each client;
- Transaction Monitoring: The Bank maintains full knowledge of all the transactions conducted in its premises, acting in a preventive way as to suspicious transactions and/or situations which may be directly or indirectly connected to the crimes related to money laundering or terrorist financing;
- Screening: The Bank automatically screens all clients, group companies, affiliates, beneficial owners and authorised signatories against the official restrictive lists, blacklists, PEP lists, adverse media lists and sanction lists;
- In addition to paying close attention to transactions, officers and staff must observe carefully those of doubtful source or which are incompatible with the economic-financial capacity of the client, or their connections and relationships with other corporations, individuals or third parties;
- The written explanation recorded by the account officers on the unusual transactions indicated in the transaction verification routines must be based on elements which support and substantiate the transaction(s), by means of an effective and thorough data collection and customer file research;
- The contacts and visits to customers with a view to obtaining information and clarifications on their transactions must always be conducted by the Relationship Manager's team with commercial skill and focus, taking the opportunity to continually update customer data;
- The establishment or maintenance of a relationship with a customer must always be guided by the perspective of transparency and honesty of the customers activities, according to the Know-Your-Customer principle, and not only by the commercial interest and/or profitability this customer may provide in its relationship with the Bank;
- The identification of a proposal or of an effective transaction or situation with evidence of money laundering or terrorist financing, must be immediately reported to the Chief Compliance Officer which, after the pertinent analysis, will determine if the transaction requires reporting to the FIU authorities;
- The Officers, Managers and staff must keep confidentiality on the reports made and, under no circumstances, may disclose or reveal the occurrence to customers or the people involved;

- In regards to records relating to client information and transactions, the Bank retain records concerning client identification, verification and all transactions as evidence of work undertaken in complying with the Laws and Regulations. The records are retained for a period of at least 5 years after the completion of all one-off transactions or the ending of a business relationship;
- The Bank undertakes to provide AML training to all members of staff on an annual basis. The Bank uses a combination of e-learning platforms and face to face classrooms for the AML/CTF employee training.