

26 September 2023

Anti-Money Laundering/Combating the Financing of Terrorism Statement

Luxembourg is one of the charter members of the Financial Action Task Force on Money Laundering (FATF) and a member of the European Union, is subject to EU regulations concerning Anti-Money Laundering and Combating the Financing of Terrorism (“AML/CFT”).

Eurobank Private Bank Luxembourg S.A. (the “Bank”), established in Luxembourg, is subject to the Luxembourg legal framework on the prevention and the fight against money laundering and terrorism financing. The Bank is supervised by the Commission de Surveillance du Secteur Financier (the “CSSF” or the “Regulator”). As evidence for its licence as a regulated Bank, please refer to the CSSF website: www.cssf.lu.

Our Bank strictly complies with the laws and regulations on the prevention of money laundering and terrorism financing, as well as with the Circulars and Regulations issued by the CSSF from time to time.

AUDIT AND MANAGEMENT VALIDATION

In accordance to the legal framework, the Bank has implemented a compliance function, responsible for the elaboration of an AML/CFT program. This program (approved by the authorised Management of the Bank and the Audit Committee) and its respective implementation are checked by the external audit firm on a yearly basis and results are reported (if any) to the Regulator.

In addition, procedures and practices are audited by an independent internal audit function. In compliance with such rules, our Bank has elaborated, and continuously adapts and improves, its respective procedures and policies.

PROCEDURES

The Bank has in place an AML/CFT Policy and Manual approved by the authorised Management of the Bank as well as the Audit Committee and ultimately ratified by the Board of Directors, The purpose of which is to describe the Bank’s internal control framework for AML/CFT and Sanctions based on applicable legal and regulatory requirements as well as best practices.

The Board of Directors has overall responsibility for having in place an appropriate framework for compliance with laws and regulations, and an effective control system, which allows for ML/FT and Sanctions risks to be assessed and managed appropriately.

CUSTOMER DUE DILIGENCE ('CDD')

The Bank applies the "Know your Customer" (KYC) and CDD principles which constitute the basis of all AML/CFT and Sanctions compliance procedures including the collection and maintenance of adequate information, knowledge of the Customer and Customer's transactions and use of products throughout the lifecycle of the Business Relationship

The Bank does not establish a Business Relationship, or carry out any transactions, in cases where the identity of the Customer cannot be satisfactorily established and verified, including beneficial owners where applicable and documentary evidence of their identification paper is held. Thus, the Bank shall ensure that it has satisfactory knowledge of the Customer and its business activities.

For the purpose of preventing, detecting and investigating Unusual and Suspicious Transactions concerning possible money laundering or terrorist financing, the Bank is legally bound to keep all the documents related to the client's files and transactions for at least five years after the end of the business relationship.

SPECIFIC ENHANCED DUE DILIGENCE

High risk clients and Politically Exposed Persons

Business relationships with high risk clients and Politically Exposed Persons (as well as their family members and close associates), if any, are covered by Policy and Manual consistent with legal requirements and industry best practices.

Shell banks

Our Bank prohibits accounts/relationships with "shell banks" (i.e. a foreign bank without any physical presence in any country and that is unaffiliated with a regulated financial group).

COOPERATION WITH AUTHORITIES AND SUSPICIOUS TRANSACTION REPORT

In the context of preventing the financing of terrorism and complying with embargoes and restrictive measures, the Bank has in place a real-time monitoring tool of all sender/receiver data of transactions against national and international sanctions lists (UN, EU, OFAC, CSSF, HMT, BIS and DFAT) ensuring that clients' files and transactions are checked on a daily basis.

The Bank carries out daily name screening CDD by filtering customer data registered in its Customer Data Management application against the sanction/watch lists of the World Compliance database.

In accordance with applicable laws and regulations, including privacy and data protection laws, our Bank fully co-operates with governmental and law enforcement authorities. We are strictly complying with any information request from those authorities to which client information and documentation may be made available upon request.

BRANCHES AND SUBSIDIARIES

As required by applicable laws and regulations, our AML/CFT Policy and Manual apply to our subsidiary, branch and representative office, and to any other future entity of the Bank falling under the provisions of the Policy and Manual.

AML/CFT TRAINING

All Staff, including the members of the management body and the authorised management must complete the AML/CFT and Sanctions training on a yearly basis in order to ensure that they possess an adequate awareness level of the risks related to ML/FT and Sanctions according to their roles and responsibilities. New Staff are required to attend a training within 30 days of being hired.

The present statement reflects current legal obligations incumbent to the Bank that reserves the right to adapt its Policy and Manual at all times with the legal or regulatory framework and professional guidelines.



Helen FOTINEAS
Vice – President



Danielle MARC
Chief Compliance Officer

