ALPHA BANK

Synopsis of the ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) POLICY
(As approved by the Bank's Board of Directors on 27.02.2025)

GROUP POLICY FRAMEWORK

Money laundering (hereinafter ML) is the process by which criminals conceal the illegal origin of their property or income.

Terrorist financing (hereinafter TF) is the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used in order to carry out any of the terrorist offences.

The solvency, the integrity and the reputation of the Bank and of the Group, as well as the reliability of the financial system in general, may suffer greatly as a result of the efforts made by criminals to commit any ML/TF offence. The Bank, taking into account the AML/CFT regulatory framework in whole, including EBA Guidelines, the FATF Recommendations and its Compliance Risk Appetite Statement, applies at Group level the present AML/CFT Policy, which has been approved by the Bank's Board of Directors. The Policy is reviewed, annually, or earlier, if necessary.

The Group Companies and Branches of the Bank operating in Greece and abroad implement the current AML/CFT Policy by laying down specialised procedures and installing appropriate IT systems.

More specifically:

The Procedures:

- Are adapted to the nature of the business activities of each Group Company and comply with the applicable local regulatory framework.
- Are periodically evaluated and revised when deficiencies are identified or where the need for their adjustment arises.
- Are approved by the Management or the Board of Directors of the Group Company and are communicated to the Employess, whose roles and responsibilities are clearly allocated.

The IT Systems:

- Are appropriate to provide timely and reliable Customer and transaction monitoring against the sanction lists.
- Allow continuous monitoring with regard to the business relationship, including a thorough examination of the transactions and activities of the Customer and of its beneficial owner(s), throughout the duration of the business relationship.
- Are subject to regular update in order to effectively address risks that originate from changes in the characteristics of the existing and new Customers, products and services.

The key components of the AML/CFT Policy are the following:

- The role and responsibilities of the management body and the AML/CFT Compliance Officer in the AML/CFT framework
- The ML/TF Risk Assessment
- Customer Due Diligence
- Remote Customer onboarding
- Customer periodic review on ML/TF risk
- Reporting of suspicious/unusual transactions
- Compliance with sanctions and restrictive measures against countries, persons or entities

- Compliance with other obligations provided for in the legal and regulatory framework.

ROLE AND RESPONSIBILITIES OF THE MANAGEMENT BODY AND THE AML/CFT COMPLIANCE OFFICER, IN THE AML/CFT FRAMEWORK

The Audit Committee is responsible for overseeing and monitoring the implementation of the internal governance and internal control framework to ensure compliance with applicable requirements in the context of the prevention of ML/TF.

The Board of Directors implements the appropriate and effective organisational and operational structure necessary to comply with the AML/CFT strategy; ensures implementation of internal AML/CFT policies and procedures; reviews the AML/CFT Compliance Officer's activity report; ensures AML/CFT reporting to the competent authority; and, where operational functions of the AML/CFT Compliance Officer are outsourced, ensures compliance with the outsourcing arrangements.

The Group Chief of Compliance is responsible for ensuring that the Group's obligations, as a whole, regarding the prevention of the use of the Financial System for ML/TF are met.

ML/TF RISK ASSESSMENT

Following the Risk Based Approach (RBA), Group Companies take a holistic view of the ML/TF risks to which they are exposed, by identifying and assessing the ML/TF risk associated with the products and services they offer, the jurisdictions they operate in, the Customers they attract and the transaction or delivery channels they use to service their Customers.

The Group Companies classify the Customers, into at least three risk categories: low, medium or high. The categorization is accompanied with the corresponding due diligence measures (simplified, standard,or enhanced).

In the unacceptable risk category where the establishment of a new relationship is not allowed, and any existing business relationship is terminated, specific Customer categories are included such as persons subject to restrictive measures or crypto-asset issuers and crypto-asset service providers without the necessary authorization.

CUSTOMER DUE DILIGENCE

The overall risk assessment as well as the individual risk assessment, requires the Group Company to identify the points where it focuses its actions in the context of ML/TF, both when onboarding accepting a new Customer and throughout the duration of the business relationship. The CDD measures to be taken include the following:
(a) identification and verification of the Customer's identity,
(b) the verification of the identity of the beneficial owner,
(c) the creation of a financial/transactional profile of Customers,
(d) the scrutiny of any transaction or activity, and the exercise of continuous monitoring.

REMOTE CUSTOMER ONBOARDING

The Group Company has put in place and maintains policies and procedures regarding remote Customer onboarding process and also monitors this process.

CUSTOMER PERIODIC REVIEW ON ML/TF RISK

As part of the implementation of due diligence measures the Group Company periodically reviews Customers for their ML/TF risk, taking into account the scope and nature of their business relationship, as well as their transactional activity and financial profile.

REPORTING OF SUSPICIOUS/UNUSUAL TRANSACTIONS

Upon detection of suspicious or unusual transactions that are not justifiable based on the existing information, said transactions are reported to the competent FIU.

The report is submitted as per the provisions of the local regulatory framework and the internal procedures of the Group Company, applying the protection measures for reporting parties.

COMPLIANCE WITH SANCTIONS AND RESTRICTIVE MEASURES AGAINST COUNTRIES, PERSONS OR ENTITIES

The Group Company monitors the regulatory framework at Group level, as to achieve full compliance with regulations issued by the European Union and the United Nations Security Council on restrictive measures and sanctions against countries, persons or legal entities, concerning customers, transactions, services and products. Restrictive measures imposed by the US Government Services (OFAC), or the United Kingdom (His Majesty's Treasury - HMT) are taken seriously into consideration when the corresponding risk is assessed.

COMPLIANCE WITH OTHER OBLIGATIONS UNDER THE LEGAL AND REGULATORY FRAMEWORK

The effective implementation of AML/CFT Policy is based on complete and up-to-date training programmes that respond to ever-changing conditions. Each Group Company provides annual training programmes, to its staff.
Furhermore, all details and information collected are kept in printed or electronic form for a period of five (5) years after the end of the business relationship with the Customer or the date of the occasional transaction. Upon expiry of that period, the Group Company shall delete the personal data, unless their keeping for longer periods, which may not exceed ten (10) years, is permitted or reasonably required by any other law or regulation. Moreover, the Group Company providing payment services apply Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain Crypto-assets and repealing Regulation (EU) 2015/847.

.