Anti-Money Laundering (AML) Policy

CONFIDENTIALITY
Public

IDENTIFICATION

Document History

Version	Date	Elaborated	Revised	Approved	Revision Comment
FIN.0013.01	2021.12.17	Eduardo Cruz (RCC)	Carina Ramos (FIN)	Renato Oliveira (CEO)	Original Version
FIN.0013.02	2023.07.31	Eduardo Cruz (RCC)	Renato Cardoso (CCID) Carina Ramos (FIN)	Renato Oliveira (CEO)	Revision after PWC Gap analysis.

Porto, 31st July 2023

Renato Oliveira

João Lima Pinto

Update and approval

This Anti-Money Laundering (AML) shall be updated if deemed necessary, whenever there is a need or requirement to do so. This instruction shall be updated in respect of changes within business requirements or other regulatory changes, changes in the market where ebankIT operates, and internal changes. Any changes to this AML Policy are subject to approval by the Board of Directors.

INDEX

INTRODUCTION AML POLICY

This Anti-Money Laundering Policy (AMLP) is adopted by ebankIT - Omnichannel innovation, S.A. (the "Company", “ebankIT” or "we").

ebankIT is subject to EU and Portuguese anti-money laundering laws, including Law n.º 87/2017, dated as of August 18th and the Portuguese Criminal Code (together the “AML Laws”).

In general, money laundering refers to transforming the proceeds from illegal activities into the legitimate economy, by hindering the retracement of the real source of the proceeds and concealing the illegal origin of the money, goods or other benefits. It is defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. It can often be seen in connection with very serious types of crimes, including drug trafficking, terrorism, corruption, and tax evasion.

Examples of types of fraudulent activities include insider trading, market manipulation, Ponzi schemes, cybercrime, and other investment-related fraudulent activity[1].

Corruption undermines legitimate business activities, distorts competition, and exposes companies and individuals to high risks. ebankIT is opposed to all forms of corruption, irrespective of which country where it operates, and adheres to the Portuguese anti-corruption applicable laws provided in the Portuguese Criminal Code and in other statutory law. Corruption can take many forms but most often it occurs through bribery.

Bribery is generally defined as offering, promising, giving, accepting, or soliciting of an undue advantage of any value (which could be financial or non-financial), directly or indirectly, and irrespective of locations, in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the performance of that person’s duties.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as, or similar to, methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

---

[1] *See art.º 368.º-A Código Penal Português*
Branqueamento de capitais e financiamento do terrorismo | Banco de Portugal (bportugal.pt)

ebankIT AML policies, procedures and internal controls are designed to ensure compliance with all applicable laws and regulations, and are also in place to account for both changes in regulations and changes in ebankIT' s business.

This AMLP consists of the following ebankIT's internal documents:
• Code of Ethics and Business Conduct;
• Anti-Corruption and Conflict of Interest Policy;
• Reporting Channel Privacy Notice;
• Prevention Plan for Risks of Corruption and Related Infractions;
• Third-parties Management Policy;
• Statement of Non-Conflict of Interest Form;
• Commitment Term Form.

TO WHOM DOES THIS POLICY APPLIES

This AMLP applies to all ebankIT´s employees and collaborators and provides a standard guideline for what is required from everyone at ebankIT.

ebankIT also expects its suppliers, contractors, consultants, and other business partners to follow these same principles when dealing with ebankIT.

Every ebankIT's employees and collaborators are expected to be fully committed to conduct business ethically and in compliance with the applicable laws and regulations that apply in the markets where ebankIT operates.

RESPONSIBLE FOR ANTI-MONEY LAUNDERING AND TERRORISM FINANCING

ebankIT's ExCom (Executive Committee) has appointed the following responsibilities:

- Heads of Departments are responsible for collecting due diligence evidences;
- Finance Department for managing repository of evidences;
- Compliance and Continuous Improvement Department for monitoring the adequacy of the applicable regulatory framework;
- Compliance and Continuous Improvement Department for conducting internal annual audits.

CONTACT INFORMATION

If you have any questions about this AMLP, you may contact the Compliance and Continuous Improvement Department using the following e-mail: compliance@ebankit.com.

MAIN PRINCIPLES

ebankIT assumes the duty to combat money laundering and the financing of terrorism through the observance, within the scope of its performance, with principles and good practices, ensuring the effective application of those procedures and controls. In particular, the following procedures shall occur prior to any financial acts (financial transactions).

ebankIT is firmly opposed to all forms of money laundering, and complies with all applicable AML laws, taking steps to prevent its financial transactions from being used by others to launder money.

PROCEDURES

VERIFYING INFORMATION

ebankIT uses risk-based procedures to verify the accuracy of the information about third-parties, at reasonable and practicable extent, to ensure having legitimate information that supports the decision making.

ebankIT informs all third-parties like clients, suppliers, contractors, consultants and other business partners about its AMLP and due diligence procedures, to ensure that all follow these principles when dealing with ebankIT.

DUE DILIGENCE

Identifying representatives and beneficial third-parties owners.

Prior to the establishment of a business relationship, Heads of Department take due diligence for future financial acts with the purpose of identifying representatives, shareholder structure and beneficial third-parties' owners according to law requirements and to clarify the legitimacy or legality of the acts.

This identification should be done for clients with total expected annual transaction value above 100k Euros and for suppliers with total expected annual transaction value above 50k Euros (excluding organizational events companies).

Before closing an agreement with a third parties, Heads of Department shall bring evidence that the customer is legally established and conducting a law-abiding business, namely, providing the banking license certification (or equivalent). In addition, Heads of Department shall procure clear evidence that the signees identified to execute the agreement on behalf of the third parties are legal representatives and therefore own legal authority to bind the client for the agreement act.

Sanctions consultation

Heads of Departments should consult sanctions list bellow to ensure the legality of the act:

https://sanctionssearch.ofac.treas.gov/

https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en

Politically Exposed Person

If, during the above-described consultation and before executing a financial act, Heads of Department identify a "PEP" - Politically Exposed Person, then, they should present and obtain, from the identified PEP, signature of the HRM.033 - Commitment Term, that engages the PEP to comply with ebankIT Code of Ethics and Business Conduct.

Additional information

During the due diligence process, other information related to codes of conduct, management policies and procedures may need to be requested by Heads of Departments.

Heads of Departments that are responsible for the procurement of a future financial act should provide a positive or negative opinion on the progress of the due diligence process. This enables the respective Board Member to identify potential risk situations and those in which ebankIT may not go ahead with the business deal.

Examples of situations where the decision may be to deny any future financial act by interrupting potential business deals (among others - list not exclusive):

- When a third-party does not give guarantees that the information provided is reliable.
- When a third-party is listed in the public lists of companies / persons sanctioned by the competent authorities.
- When there's a suspicion of a third-party being involved in acts of corruption. (For this matter, refer to ebankIT Anti-Corruption and Conflict of Interest Policy).

The business relationships may be periodically reviewed, in order to ensure that the information remains accurate and up to date. The decision process of all third-parties in business with ebankIT must consider the risk classification and the implementation of extraordinary proceedings when a particular suspicion arises.

All evidence provided by third-parties should be recorded on Sharepoint\FINDD\Area\Name, namely:

- Identification of representatives, shareholder structure and beneficial third-parties' owners;
- Banking license or equivalent;
- Print screen from sanctions analysis;

- Document that certifies the binding authority conferred to representatives that are appointed to sign agreements on behalf of the company;
- HRM.0033 - Commitment Term signed by PEP;
- Other necessary evidences.

ebankIT ensures a safe and longstanding method of documental archiving and conservation for this purpose.

The decision and the reasons regarding approval or refusal must also be stored in this repository. An email with this information with knowledge of a Board member should be enough.

The ISM.0007 - Third parties List (above v.06) is driven to follow up third parties risk level and performance by recording demerits. It must be updated with any constrains and change management.

RELATIONSHIP WITH SUPPLIERS, BUSINESS PARTNERS AND CLIENTS

ebankIT encourages its employees and collaborators to build and maintain relationships with its suppliers, clients, and business partners always with integrity in respect of applicable laws and ebankIT's internal rules presented on "Code of Ethics and Business Conduct" and on Anti-Corruption and Conflict of Interests Policies in which are mentioned the risks and actions to take into consideration to prevent situations of AMLTF.

Special care should be exercised during negotiations, decision-making processes, bids, tenders, and similar processes.

NON-DISCLOSURE

At no time, ebankIT or any of its employees and collaborators may disclose to their clients, suppliers, partners or third-parties the information that have been or will be made available to the competent authorities or to the internal or judicial investigations that could be in progress.

SANCTIONS

Violations of Anti-Bribery and AML Laws will not be tolerated and ebankIT will take steps to sanction any unlawful conduct attributable to ebankIT's employees and collaborators and/or third-parties, which may emerge as a result of internal verifications or whistleblowing reports, according to ebankIT Code of Ethics and Business Conduct and specific laws and regulations.

AML COMPLIANCE MONITORING AND REPORT

ebankIT provides specific, independent, and anonymous channel to treat any violations regarding this AMLP and any legislation and regulations in force.

All employees and collaborators are expected to be vigilant and to play an active part in the Anti-Bribery, the Anti-Corruption and AML activities.

Any suspected or known violation of the Anti-Bribery, Anti-Corruption or AML Laws or relevant sections of this Policy must be promptly reported through ebankIT reporting channel on the website: www.ebankit.com.

EBANKIT INTERNAL CONTROL

ebankIT ensures the compliance with this policy promoting awareness to maintain a culture that fosters a positive and constructive attitude towards risk management on AML matters.

Annually a specific internal audit to this Policy by Compliance and Continuous Improvement Department is conducted.

Within 5 years all entities within the scope of this policy shall be audited, according to what is defined in this procedure.

When entities with financial acts raise suspicions of inappropriate conduct, documentation on repository should be reviewed and audited.

Also annually an audit to ebankIT financial statements, in accordance with the Accounting and Financial Reporting Standards adopted in Portugal under the Portuguese National Accounting System (SNC) is conducted.

TRAINING

To have a high level of awareness among employees and collaborators with regards to corruption, bribery and money laundering, ebankIT ensures specific and regular training of the most concerned staff.

To raise awareness of AML and Anti-Corruption and Anti-Bribery issues, training sessions are regularly performed to foster knowledge of the obligations arising from the law.

In the case of new employees and collaborators, ebankIT provides upon admission, appropriate training on policies, procedures, and internally defined controls.

UPDATING AML POLICY AND PROCEDURES

Policies and procedures are reviewed when deemed necessary by Compliance and Continuous Improvement Department.