Anti-money Laundering and Know Your Customer Policy

v.1.2 July 20th, 2020 *Apostloris, Unipessoal Lda*

1. Introduction

The purpose of the Anti-Money Laundering and Know Your Customer Policy (also the "AML&KYC Policy") is to identify, prevent and mitigate possible risks of Apostloris, Unipessoal Lda being involved in any illegal activity.

In conformity with European, Portuguese and international regulations Apostloris, Unipessoal Lda has implemented effective internal procedures to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to react correspondingly in case of any form of suspicious activity involving our clients.

2. Accepted jurisdictions

Apostloris, Unipessoal Lda crypto services are available only for the residents of the European Economic Area (EEA) that maintain a checking account in good standing in one of EEA-operating SEPA-licensed banks and possess a valid EEA member state issued national ID card or passport.

Importantly, U.S. citizens and legal residents including those in possession of valid EEA-issued ID documents as well as U.S. registered legal entities are explicitly barred from using any of our crypto services.

3. Policies

The AML&KYC Policy includes identity verification procedures, Compliance Officer, internal training, transactions monitoring and risk assessment. Customer due diligence ("CDD") has become one of one of the international standards for preventing illegal activity including money laundering. Thus, Apostloris, Unipessoal Lda has implemented its own verification procedures within the rigorous standards of anti-money laundering and "Know Your Customer" and "Customer Due Diligence" procedures.

4. Identification

The identification procedure requires the client to provide us with reliable, independent sourced documents, data or information.

A valid EEU member state issued identification is mandatory, while additional documents that meet the criteria below will be requested by the Compliance Officer at their discretion.
Accepted ID documents are:
1) A national EEU ID card;
2) An EEA member state issued passport.
Accepted support documents are:
1) A bank statement with the client's full name, address and date (last 90 days);
2) A utility bill with the client's full name, address and date (last 90 days).
We reserve the right to request any other document(s) not listed below in case of any doubt or suspicion as well as in case of the positive "high risk" individual detection by any of our screening checks described below.

We reserve the right to collect and retain the identification information for the purposes of AML&KYC Policy compliance.
We will take steps to confirm the authenticity of documents and information provided by clients. All legal methods for double verification of identification information will be used, and we reserve the right to investigate the cases of certain clients whose identities have been identified as dangerous or suspicious, so called "high risk" individuals.
In addition, we require that all clients provide a copy of signed declaration of cryptocurrency purchase or electronic equivalent for each operation.

Moreover, we reserve the right to verify the identity of the client on an ongoing basis, especially when its identification information has been changed or its activities appear suspicious or unusual for a particular client. In addition, we reserve the right to request from the client current documents, even if they have been authenticated in the past.
As part of our record retention policy, all provided documents and additional information about the client will be collected and stored for 10 consequent years, shared and protected strictly in accordance with the Portuguese law, GDPR, our Privacy Policy and anti-money laundering requirements by the Bank of Portugal.

After confirming the identity of the client, we will refuse potential legal liability in a situation where our Crypto Services are used to conduct suspected or confirmed illegal activities.
Additionally, we will refuse any services to individuals identified as Politically Exposed Persons (PEPs) or legal entities of which they are ultimate beneficial owners (UBO).

In addition to identifying the executive representative according to the requirements listed above, all legal entities must be registered in the EEA, be in good standing and provide documentation necessary to disclose their ultimate beneficial ownership (UBO) information in order to be eligible for our crypto services offering.

Apostloris, Unipessoal Lda explicitly prohibits deposits from “shell” banks and requires all wire transfers to be performed with an EEA registered bank holding a valid SEPA license.

4. Compliance Officer

The Compliance Officer is the person, duly authorized by Apostloris, Unipessoal Lda, whose duty is to ensure the effective implementation and enforcement of this AML&KYC Policy.

It is the Compliance Officer’s responsibility to supervise all aspects of our anti-money laundering and counter-terrorist financing, in particular collecting clients’ identification information, establishing and updating internal policies and procedures for the completion, review, submission and retention of all reports and records required under the Portuguese law and regulations, monitoring transactions and investigating any significant deviations from normal activity, implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs, updating risk assessment regularly, providing law enforcement with information as required under the applicable laws and regulations.

The Compliance Officer is entitled to interact with law enforcement, which are involved in prevention of money laundering, terrorist financing and other illegal activity in Portugal and overseas.

5. Internal Training

The Compliance Officer conducts monthly training sessions for relevant employees, focused on successful client identification, transaction monitoring, including the set of criteria to identify higher risk transactions and suspicious user activity.
The training sessions also include overview and practical examples of common money laundering practices, red flags to identify those and how to report such activities to the local law enforcement agencies.
Extraordinary training sessions are held in case of updated AML polices, changes in relevant legislation or any new significant information that can be used to improve our anti-money laundering practices.

Attendance records and presented training materials are retained internally.

6. Additional control and verification measures

The clients, both natural and legal persons, are known not only by verifying their identity but also by analyzing their transactional and behavioral patterns. Therefore, we rely on big data analysis as a risk-assessment and suspicion detection tool.
We perform a variety of compliance-related tasks, including capturing data, filtering, record- keeping, investigation management, and reporting.

Such functionalities include:
1) Initial check of all clients against recognized black and sanctions lists (OFAC SDN, FSF, enterprise sanctions lists, domestic lists);
2) Consequent daily checks of all clients against recognized black and sanctions lists (OFAC SDN, FSF, enterprise sanctions lists, domestic lists), aggregating transfers by multiple data points, placing clients on watch and service denial lists, opening cases for investigation where needed, sending
3) Additional screening against the watchlist issued by the government of Portugal;
4) Case and document management and retention system;
5) Internal audit on monthly basis to make sure all the described procedures are functioning properly and records are up-to-date.

7. Transactions monitoring

In connection with this AML&KYC Policy, the following apply:
1) We will monitor all transactions and report the transactions of suspicious nature to the proper law enforcement through the Compliance Officer;
2) We will identify higher risk transactions and notify the Compliance officer to take additional measures to verify their nature and status;
3) We will request the client to provide additional information and documents for such transactions;
4) We will suspend or terminate any operations for the client when we have suspicion that this client ever engaged in any illegal activity;

The above list is by no means exhaustive, however, and the Compliance Officer will monitor all clients' transactions on a regular basis in order to define whether such transactions are to be reported to the law authorities and treated as suspicious or are to be treated as bona fide.

8. Risk assessment

Apostloris, Unipessoal Lda, in line with the European, Portuguese and international requirements, has adopted a risk-based approach to combating money laundering and terrorist financing.

Our services are not available outside of the European Economic Area (EEA). Therefore, our risk assessment measures are focused on identifying locations within the EEA area, as a whole highly secure, that could be associated with transactions of higher risk, as well as identifying and reporting individual from “high risk” countries that may be of possession of EEA issued identification documents.

All identified higher risk individuals and transactions are subject to extensive scrutiny by the Compliance Officer and multiple automated software-based verifications.

By adopting a risk-based approach, we are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks.

Any operation that is deemed as posing risks by the automated monitoring or the Compliance Officer will be declined swiftly and reported to the law enforcement authorities.