AML (Anti Money Laundering) policy

PayNox EOOD

ID number: 208071994

Legal address: Bulgaria, City of Burgas, 19 Marahydyk St., fl. 2, office 1

LAST UPDATED ON: 23.12.2024

This document is for internal purposes only, and should not be shared with any physical or legal entities outside of the company except the cases when it is specially required and upon approval of the Company’s director.

Caution: This document contains confidential information, and no parts of it may be duplicated or saved in print or electronic form without the owner of the document's consent.

Director:

TABLE OF CONTENTS

1.INTRODUCTION AND DEFINITIONS

"PayNox" EOOD (LLC) (may also be referred to as “the Company”, “we”, “us” in this policy) is a legal entity duly incorporated in Bulgaria which carries out activities in the field of exchange services between virtual currencies and non-gold-backed recognized currencies and is registered in The electronic public register of entities engaged in providing services for the exchange of virtual currencies and recognized currencies without gold backing, services for the transfer or exchange of virtual assets, services for the storage and management of virtual assets, enabling control over such assets, and services related to the public offering of virtual assets, as well as providers of wallets offering custodial services. The Company understands that its activity is related to virtual assets and therefore has a higher risk of money laundering due to misuse by clients. Thus, it is a primary Company’s goal to establish and follow appropriate rules to fight against these potential risks.

The purpose of the policy is to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements under the following regulatory acts:

- Anti-Money Laundering Measures Act (AML Act),
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC,
- Criminal Code of Bulgaria,
- the recommendations developed by the Financial Action Task Force (FATF),
- and other legislation.

The objectives of the Anti-Money Laundering (AML) policy are to establish a comprehensive framework that prevents the misuse of the Company’s services and products for money laundering and terrorist financing activities.

The Company is committed to ethical standards of business conduct and adopts a zero-tolerance approach to financial misconduct, including money laundering.

Money laundering refers to the deliberate actions of:

1. Converting or transferring property, knowing that the property was acquired through criminal means or involvement in a crime, with the intent to conceal or hide the illegal origin of the property, or to assist a person involved in such an act in order to avoid the legal consequences of their actions;

2. Concealing or attempting to conceal the nature, source, location, movement, rights over, or ownership of property, knowing that the property was acquired through criminal means or as a result of involvement in a crime;

3. Acquiring, possessing, holding, or using property, with knowledge at the time of receipt that it was obtained through a crime or as a result of involvement in a crime;

4. Participating in any of the actions described in paragraphs 1-3, or conspiring to commit such an act, attempting to commit it, or assisting, instigating, facilitating, or advising in the commission of such an act or its concealment.

Money laundering also occurs when the crime from which the property was obtained was committed in another member state or in a third country and falls outside the jurisdiction of the Republic of Bulgaria.

These actions can be performed through the ultimate beneficial owner.

Ultimate Beneficial Owner is the person who enjoys the benefits of ownership or control of an entity, even if the legal ownership is held by another party. This includes individuals who hold at least **25% of the shares or voting rights** in a company, either directly or indirectly. If no individuals meet this criterion, senior management officials may be considered as UBOs.

A controlling person refers to any individual who has the authority to control or influence the decisions of a legal entity. This may include individuals who exercise significant influence over the management or policies of a company without necessarily holding formal ownership stakes.

In some cases, the Company might deal with Politically Exposed Persons (PEP) that increase the level of risks from AML perspective. For the purpose of this Policy, PEP is an individual who holds a prominent public position, such as heads of state, senior politicians, judicial or military officials, and executives of state-owned enterprises etc. Due to their positions, PEPs are considered to pose a higher risk for potential involvement in bribery and corruption, which necessitates enhanced due diligence measures by financial institutions and other obligated entities. As stated in AML law, the person is considered to be PEP even one year after the termination of its function.

Measures to prevent money laundering include:

- Comprehensive customer due diligence;
- Collection and preparation of documents and other information in accordance with the conditions and procedures prescribed by law;
- Retention of documents, data, and information collected and prepared for the purposes of this law;
- Risk assessment of money laundering and terrorist financing;
- Disclosure of information about suspicious operations, transactions, and clients;

- Disclosure of other information in accordance with the law;
- Monitoring the activities of obligated persons.

2. CORE PRINCIPLE OF THE POLICY

To effectively combat and prevent of Money Laundering (ML) and Terrorist Financing (TF) (further referred to as “ML/TF”), it is crucial to set the standards within the Company.

The following principles are used as a cornerstone for combating illegal activity when it is connected to the services of the Company:

- **Risk Based Approach (“RBA”)** is used while assessing the ML/TF risks to the Company.

This Risk Assessment identifies and assesses risks arising from the legalization of proceeds of crime and financing of terrorism that may potentially occur in the Company within the scope of provision of virtual assets services.
The norm in the fight against ML/TF has been the application of the so-called risk-based approach. The AML Act prescribes the required minimum of obligations that must be fulfilled.

In relation to this Risk Assessment and pursuant to the AML Act, Company will fulfil the following obligations:

(a) to prepare and approve this Risk Assessment
(b) to apply measures to reduce the ML/TF risks listed in this Risk Assessment
(c) to carry out internal supervision and monitoring of compliance with legal regulations
(d) to check responsible persons
(e) to update this Risk Assessment periodically.

The Company will use the following sources in the process of ML/TF risk identification and assessment:

(a) Sector analyses from the sphere of ML/TF (especially by FATF-GAFI)
(b) National risk assessment processed in compliance with Section 30a of the Act1
(c) European risk assessment processed by the European Commission
(d) Sources considered by the National Bank
(e) other regulations.

A risk-based approach (RBA) to Anti-Money Laundering (AML) policy is a strategic framework that prioritizes the identification, assessment, and mitigation of risks associated with money laundering and terrorist financing. This approach allows financial institutions and other obligated entities to allocate their resources more effectively by focusing on higher-risk areas while applying simplified measures to lower-risk situations.
Under an RBA, The Company categorizes clients based on their risk profiles, which allows them to apply different levels of due diligence. Low-risk clients can be onboarded quickly with minimal

verification requirements, reducing friction and enhancing customer experience. In contrast, higher-risk clients will face additional scrutiny, which may include extensive documentation and background checks. By focusing resources on higher-risk clients, institutions can allocate compliance resources more effectively.

- Customer due diligence procedures, including enhanced due diligence measures are based on the RBA and the higher the risk, the more detailed information customers are required to submit in order to make sure that no illegal activity is taking place while the Company is providing its services;
- Maintaining risk-based systems and procedures for monitoring of ongoing customers' activity;
- Understanding that reporting suspicious activity internally and externally to the relevant law enforcement authorities (goAML and Financial Intelligence Directorate under the State Agency for National Security (FID-SANS, Bulgarian FIU or FIU) is crucial to combat ML and TF risks;
- Record keeping for the minimum prescribed periods is maintained at all times, including records regarding internal investigations and external reporting;
- Training and screening of the relevant responsible persons as well as providing most recent information about AML and counter-terrorism financing (CTF) legislation to keep the awareness of such responsible persons at sufficient level at all times.

3. INTERNAL CONTROL SYSTEM FOR COMPLIANCE WITH AML AND COUNTER-TERRORISM FINANCING LAWS

The system shall include:

1. **Internal Policies and Procedures**: Clear, documented policies and procedures shall be in place to ensure compliance with AML and counter-terrorism financing (CTF) laws, including customer due diligence, transaction monitoring, and reporting of suspicious activities.

2. **Regular Risk Assessments**: The system shall conduct regular risk assessments to identify potential vulnerabilities to money laundering and terrorist financing, adapting internal controls accordingly to mitigate identified risks.

3. **Staff Training and Awareness**: Ongoing training programs for responsible persons shall be established to ensure awareness and proper execution of AML/CTF policies and procedures.

4. **Monitoring and Auditing**: The internal control system shall include regular monitoring and auditing of transactions and activities to assess compliance with legal obligations, ensuring timely reporting and rectifying any identified issues.

5. **Appointment of a Compliance Officer**: A dedicated compliance officer/anti money laundering reporting officer (AMLRO) shall be appointed, responsible for overseeing the implementation and maintenance of the internal control system and reporting directly to senior management. If the AMLRO is not appointed as a separate officer, the Director will perform the respective functions personally.

4.THE USE OF TECHNICAL MEANS FOR AML COMPLIANCE

To prevent and detect the legalization (laundering) of criminal proceeds and the financing of terrorism, the Company may implement and maintain effective technical measures in compliance with Bulgarian Anti-Money Laundering (AML) legislation, including:

1. **Customer Identification and Verification**: The platform shall use automated systems for real-time customer due diligence (CDD) to verify the identity of users and assess the risk of illicit activities.
2. **Transaction Monitoring**: Automated monitoring tools shall be employed to track and analyze transactions for suspicious activity patterns, including unusual amounts, high-frequency trading, and transactions involving high-risk jurisdictions.
3. **Suspicious Activity Reporting (SAR)**: The platform will utilize technical solutions to automatically flag suspicious transactions, ensuring prompt reporting to the Bulgarian Financial Intelligence Unit (FIU) in accordance with legal requirements.
4. **Data Retention and Protection**: Secure, encrypted systems shall be used to store and protect all customer data, transaction records, and other relevant information for a minimum of 5 years, as required by law.
5. **Risk-Based Approach**: The platform shall use risk-based algorithms to evaluate transactions and identify higher-risk clients or activities that may require enhanced due diligence.

These technical measures are designed to ensure full compliance with Bulgaria's AML regulations and to support the detection and prevention of money laundering and terrorism financing activities.

5. CUSTOMER DUE DILIGENCE AND RELATED PROCEDURES

Customer Due Diligence (CDD) is the process of identifying and further verifying the identity of customers and assessing their potential risks in relation to ML/TF.

Customer due diligence measures must be applied in the following situations:

When establishing a business relationship, including when opening an account, where the establishment of the relationship is linked to the account opening. Creation of anonymous accounts is prohibited.

When carrying out an occasional operation or concluding an occasional transaction that amounts to or exceeds the lev equivalent of EUR 15,000, or the equivalent amount in another currency, regardless of whether the operation or transaction is a single action or a series of linked operations.

When carrying out an occasional operation or concluding an occasional transaction that amounts to or exceeds the lev equivalent of EUR 5,000, or the equivalent amount in another currency, and the payment is made in cash, regardless of whether the operation or transaction is a single action or a series of linked operations.

When carrying out an occasional operation or transaction that involves the transfer of funds, as defined in Article 3(9) of Regulation (EU) 2015/847, amounting to or exceeding the lev equivalent of EUR 1,000, or the equivalent amount in another currency.

In cases where the value of an occasional operation or transaction cannot be determined at the time of its execution due to its nature, CDD measures must be applied as soon as the value is determined, if it amounts to or exceeds:

The lev equivalent of EUR 15,000 or its equivalent in another currency, irrespective of the payment method or whether the operation or transaction is single or linked.

The lev equivalent of EUR 5,000 or its equivalent in another currency, when the payment is made in cash, regardless of whether the operation or transaction is single or linked.

Key Elements of CDD are customer identification, risk assessment, ongoing monitoring, record keeping, politically exposed persons (PEPs) monitoring, sanctions and watchlist screening.

Know Your Customer (KYC) Procedures for individual clients.

The primary purpose of the KYC procedures is to:

- Identifying of all customers before allowing access to the Company's services.
- Assess the risk of each customer based on their personal profile, transaction history, and geographical location.
- Ensure compliance with local and international AML regulations to prevent the Company from being used for illicit activities.

At the point of account registration, all new customers must undergo a verification process that includes the following steps:

i. Collection of Personal Information.

The Company requires customers to provide the following information:

- Full Name: As per a government-issued identification document.
- Date of Birth: To confirm the customer's age.
- Nationality/Residence: Country of citizenship and current place of residence.
- Address: Full residential address, including postal code.
- Email Address: For communication and account-related notifications.
- Phone Number: For contact and verification purposes.

ii. Identity Verification.

The customer must provide at least one valid government-issued identification document (e.g., passport, driver's license, national ID card).

Additionally, the customer will be required to submit a selfie or liveness verification with the identification document to confirm the person is physically present.

If necessary, further documents may be requested to verify the customer's identity or address, such as utility bills, bank statements, or tax filings.

For customers identified as high-risk, including Politically Exposed Persons (PEPs) or individuals from high-risk jurisdictions, Enhanced Due Diligence (EDD) procedures will be applied (please see a details on risks profiles below).

The Company will continuously monitor customer activity and transaction patterns to identify any suspicious activities. This includes:

Monitoring for unusual transaction volumes, rapid transfers, or activity inconsistent with the customer's profile.

Keeping track of large or cross-border transactions that could suggest money laundering or other illicit activities.

Using automated tools to flag potentially suspicious activities and triggering further investigation when necessary.

To ensure that the information remains accurate and up to date, the Company will periodically review and update KYC details, including:

Annual Review: For all customers, their KYC information and risk profiles will be reviewed at least once a year to identify any changes or potential risks.

Customer Update Requests: Customers may be required to update their KYC information upon significant life changes (e.g., change of address, nationality, occupation, etc.).

The Company will request updated KYC information and documentation if there are any of the following events:

Changes in Customer Behavior: A customer's transaction activity changes significantly or becomes inconsistent with their profile.

Red Flags for Suspicious Activity: If a customer is flagged for suspicious activity, further identity verification and due diligence will be conducted.

Change in Risk Profile: If a customer is reclassified as higher risk (e.g., becoming a PEP, or moving to a high-risk jurisdiction), the Company will apply Enhanced Due Diligence (EDD) procedures.

The Company has the right to refuse service to any customer who does not meet the KYC requirements or who fails to provide adequate documentation for verification. If the Company identifies any fraudulent information or signs of money laundering, the customer's account may be terminated. Additionally, suspicious activities that cannot be satisfactorily explained may result in the suspension of the customer's account, followed by appropriate reporting to the relevant authorities.

Know Your Customer (KYC) Procedures for legal entities clients.

The purpose of KYC procedures for legal entities is to:

- Verify the legitimacy of corporate customers and ensure that the Company does not facilitate money laundering, terrorist financing, or other illicit activities.
- Ensure compliance with local and international regulations regarding anti-money laundering (AML) and counter-terrorism financing (CTF) obligations.
- Identify the beneficial owners of the legal entity, as well as any individuals with significant control or influence within the company.

The Company requires the following documents and information about the legal entity:

- Corporate Name: Official legal name of the entity, as registered with the relevant authorities.
- Registration Number and Jurisdiction: The unique identification or registration number and the country where the legal entity is incorporated or registered.
- Business Address: Registered office address, including postal code.
- Type of Entity: Information about the legal form (corporation, partnership, LLC, etc.) and a description of the primary business activities.

The Company requires detailed information on the beneficial owners of the legal entity. A beneficial owner is an individual who ultimately owns or controls the entity (either directly or indirectly), or who benefits from its assets, even if they do not hold formal ownership titles.

For each beneficial owner, the following information must be collected:

- Full Name of each beneficial owner.
- Date of Birth for individual verification.
- Nationality and Country of Residence for risk assessment.
- Percentage of Ownership or Control: The percentage of shares, voting rights, or ownership held by the individual.
- Proof of Identity: A government-issued identification document (passport, national ID, driver's license) for each beneficial owner.

The Company will also collect information on key individuals within the legal entity, including:

Directors and Officers: Information on the legal entity's directors, senior management, and anyone with significant decision-making authority.

Control and Governance Structure: The organizational structure of the entity, identifying individuals with direct or indirect control. In cases where beneficial ownership or control is complex (e.g., when ownership is held through multiple entities), the Company may request additional documentation or information to clarify the ultimate beneficial owners. The Company may also request ownership charts or legal structure diagrams to verify the true control structure.

The Company requires the legal entity to provide a clear description of its business activities. This includes:

Primary Business Operations: The main industry sector, products, or services the entity provides.

Revenue Model: How the entity generates income.

Geographical Focus: The countries or regions where the entity operates and does business.

The Company will classify each legal entity customer based on its risk profile. Factors to consider include:

Geographic Risk: The country or region in which the business operates, based on AML and CTF risks.

Business Sector Risk: The industry the entity is involved in, considering whether it is susceptible to money laundering or terrorist financing.

Ownership Structure Risk: Whether the entity's ownership structure is complex or opaque, which could make it more difficult to identify the true beneficial owners.

The Company will monitor the transactions of legal entities to ensure that they align with the entity's profile and business activities. The monitoring will include:

Large Transactions: Monitoring for large or frequent transactions that are inconsistent with the entity's typical business operations.

Cross-Border Transfers: Scrutinizing transactions involving high-risk jurisdictions, as well as complex international transfers.

Unusual Activity: Identifying suspicious activity such as sudden increases in transaction volumes, fund movements to or from unverified accounts, or transactions with no clear business purpose.

The Company will review the KYC information for legal entities periodically (e.g., annually or upon a trigger event), updating the entity's risk profile based on any changes in its business activities, ownership structure, or geographical focus.

The Company will trigger updates to KYC information if there are significant changes to the business, such as:

- Change in beneficial ownership.
- Expansion or modification of business activities.
- A significant change in the geographic regions where the entity operates.
- A change in risk classification due to new regulatory sanctions or findings.

The Company will retain all KYC-related documentation for legal entities. Records should include:

- Proof of corporate existence.
- Ownership documents and verification of beneficial owners.
- Records of all ongoing monitoring activities and transaction reviews.

If a legal entity fails to meet the KYC requirements or is found to be involved in fraudulent or illicit activities, the Company has the right to:

Refuse to onboard the entity or terminate the account.

Report any suspicious activity to the appropriate regulatory authorities.

6.ENHANCED CUSTOMER DUE DILIGENCE

The following scenarios trigger the application of Enhanced Customer Due Diligence:

- High-Risk Customers:
  - Customers identified as high-risk due to factors such as the country or region of residence (e.g., high-risk jurisdictions under FATF or EU blacklists).
  - Politically Exposed Persons (PEPs) and their family members or close associates.

    - Individuals or entities involved in complex or opaque structures, including shell companies or trusts with unclear ownership.
- Large or Unusual Transactions:
    - Transactions involving large amounts, particularly those exceeding the lev equivalent of EUR 15,000, or the equivalent in another currency, regardless of whether the transaction is a single operation or multiple linked operations.
    - Occasional operations or transactions involving cryptocurrency, where the amounts are unusually large, or where the origin and destination of the funds are not easily traceable.
    - Transactions involving anonymized or privacy-focused cryptocurrencies (e.g., Monero, Zcash) or use of peer-to-peer transfer methods.
- Unverified or Incomplete Information:
    - Customers who provide incomplete or unverifiable information during the standard Customer Due Diligence (CDD) process.
    - Customers where there is suspicion or doubt about the accuracy or adequacy of the provided information, such as discrepancies in the identification or verification documents.
- Transfers from High-Risk Jurisdictions

Cryptocurrency transfers originating from or being sent to countries identified as high risk by the EU or other relevant international bodies.

- Suspicious Activities or Transactions

Any transaction or activity that, based on a risk-based analysis, raises concerns regarding potential money laundering or terrorist financing, such as rapid or unexplained trading patterns, high-volume transactions, or irregular account activity.

For customers and transactions identified as higher risk, the following EDD measures will be implemented:

i. Verification of Identity and Source of Funds:

Collecting and verifying more detailed customer information, including a government-issued photo ID, proof of address, and, where applicable, information on the source of funds and wealth (e.g., income, employment, business activities).

For corporate clients, obtaining and verifying information about the ownership structure, the business nature, and the identities of beneficial owners.

ii. Ongoing Monitoring:

Continuous monitoring of customer transactions and activity, including a review of any unusual patterns or inconsistencies in the trading behavior.

Enhanced scrutiny of high-value transactions, including tracing the origin and destination of the funds, especially when they involve cryptocurrency exchanges or wallets with known links to illicit activities.

iii. Enhanced Risk Profiling:

Applying an enhanced risk assessment process that includes evaluating customers based on a comprehensive set of risk factors, such as political exposure, jurisdictional risk, transaction types, and historical activity.

For PEPs, a deeper investigation into the source of their wealth and business connections will be conducted.

iv. Use of Third-Party Verification Services:

Utilizing external sources, such as blockchain analytics tools, global sanctions lists, and PEP databases, to verify the legitimacy of transactions, wallets, and counterparties involved in transactions.

Approval for High-Risk Transactions.

Any high-risk transaction identified through the risk-based analysis must be approved by the compliance officer or senior management before being processed. The approval process will include a review of the transaction's legitimacy, source of funds, and potential exposure to illicit activities.

Politically Exposed Persons (PEPs) and Close Associates.

For PEPs and their close associates, a more detailed background check will be conducted, including public records searches and verification through trusted third-party sources. Additionally, transactions involving such individuals will be subject to heightened scrutiny, including approval from senior management before execution.

To ensure an appropriate level of risk assessment, a classification system has been implemented, categorizing risks into levels A, B, C, D and E.

7.POTENTIAL VULNERABILITIES AND THREATS

The Company has identified the following potential vulnerabilities (i.e., "weak spots" that may facilitate a client's abuse of the services for ML/TF) that might be faced in its activity:

(a) Client identification: a person who does not wish to be associated with the virtual assets service is interested in the services and therefore another person (appearing to be the client),

who is only the identity provider, acts on his behalf and conceals that he is acting on behalf of another person who does not actually wish to be associated with the virtual assets service

(b) Client check: a client provides false, superficial or incomplete information about the source of the financial resources because the client expects that reviewing the source of the financial resources is a very difficult or impossible process and expects the responsible person to neglect this obligation or fail to perform it appropriately;

(c) Persons against whom the Republic of Bulgaria applies international sanctions (including persons involved in terrorism) are hidden in complex and non-transparent ownership and management structures of legal entities; such client expects that to uncover the ownership and management structure of the client-legal entity and expects the Company to neglect this obligation or to perform it incompletely.

The Company has identified and assessed the following threats that might be faced in its activity:

(a) High risk: abuse of the virtual assets services as a technique for the legalization of resources originating from criminal activity, especially resources originating from tax fraud, subsidy fraud, corruption activity, breach of trust in administration others´ property, etc.

(b) Medium risk: international sanction evasion (i.e., changing the nature of and transferring property of persons subject to international sanctions)

(c) Medium risk: financing of terrorism

(d) Low risk: all other threats.

The risk factor is the characteristics of the client, the product provided to him/her, or the way in which it is provided, which increases the risk that services of the Company.

8.RISK PROFILE

The Company might be misused by the client for the purpose of money laundering or terrorism financing, based on which the client could be assigned a risk profile of the type A, B, C, D or E.

Risk profile - type A. The client could be assigned a type A risk profile (client with no risk or with minimal risk) in the absence of known risk factors to be assigned to a type B, C, D or E risk profile.

8.1.RISK PROFILE - TYPE B, C OR D

A client with a risk profile of the type B, C or D represents for the Company (a potential risk from the ML/TF perspective and therefore all the responsible persons, including the AMLRO, must pay close attention to the assessment of any suspicion character of this client's behavior and place increased demands on the accuracy of the information provided by the client during the first or ongoing review, where appropriate, to substantiate the information disclosed by a specific document.

The following risk factors relate to the type B, C or D risk profile, while on the fact whether a risk profile of type B, C or D could be assigned to the client based on the risk factors described here the responsible person will decide in accordance with a special document for a risk assessment profile of the client:

(a) the client uses services that include transaction to or from a country or territory that is identified as risky;

(b) the client requires a transaction that is unusually complex or large-volume, or involves an unusual way of trading, or the economic and legal purpose of which is not obvious;

(c) the client or its beneficial owner engages in a business or other activity that is "cash intensive" - that is, an activity that generates large amounts of cash or other valuable commodities of a purely anonymous nature, including virtual currencies (e.g., currency exchange, trade in precious metals, virtual currency, etc.);

(d) the client or its beneficial owner carries on business or other activity in the field of gambling, military industry and services, nuclear energy;

(e) in the course of business, the client or its beneficial owner handles content accessible only to adults, with the exception of products designed for direct consumption, such as cigarettes, alcohol, etc.;

(f) the client is a non-entrepreneurial legal entity whose activity is not traceable in trustworthy sources and the client has difficulty to prove its activity or proves it in such a way that doubts arise;

(g) a client who has previously been the subject of a suspicious transaction notification;

(h) a client whose behavior has previously shown some signs of a suspicious transaction but ultimately has not been classified as a suspicious transaction, although doubts remain;

(i) the client or its beneficial owner is a PEP, or the client is a person acting in the interest of such a PEP;

(k) any country of origin (including the registered office or residence) of the client, its beneficial owner or the person authorized to act on behalf of the client is a risk country from the ML-FT perspective;

(l) the country of origin of the person having direct or indirect participation in the client is a risk country from the ML-FT perspective;

(m) the country of origin of a person who is a member of the statutory body of a client, a representative of a legal entity in that body, or is in a position similar to that of a member of a

statutory body or otherwise has the possibility to apply influence at the client, being a legal entity, is a risk country from the ML-FT perspective;

(n) the client is a trust fund;(o) the ownership structure of the client is non-transparent;

(p) the behavior of the client or the person representing it is abnormal in or during the establishment of a business relationship compared to a typical client similar to it (e.g., non - standard requirements, unusual ways of transaction performance, requirements for special or complex types of representation, etc.);

(r) uncertainties arise as to the origin of the client's property or the beneficial owner's property or the funds held by the client or the beneficial owner of the client;

(s) open trusted sources (e.g., news media) indicate that the client or related persons have been or are involved in criminal or other unfair activities;

(t) there is a suspicion that the client is not acting on his / her own name, i.e., the property that is the subject of the service actually belongs to someone else and the client is only an intermediary or identity provider;

(u) the client or a related person (member of the statutory body, the beneficial owner) is linked to another client (factually or legally) whose risk profile is of the type B;

(v) another fact that, according to the information held by Company available, there is an increased risk of money laundering or terrorist financing associated with the client's business activity and its beneficial owner;

(w) according to the information held by Company available, there is an increased risk of money laundering or terrorist financing related to the high client’s turnover;

(x) the payment or other service used by the client, or its nature or the nature of individual transactions, is non-standard for the given type of client;

(y) any of the factors listed above, if it occurs in a legal entity in which the client has a direct or indirect participation, or otherwise has the opportunity to exercise influence over it.

8.2.RISK PROFILE - TYPE E

A client with a risk profile of the type E represents for the Company a high risk in terms of money laundering and terrorist financing. If the client is assigned a risk profile of the type E, the client will not be provided with a virtual assets service or a business relationship with the client, or the business relationship with him will be terminated and no other service will be provided.

In this situation, the client is considered to no longer meet the client's acceptability criteria.

In this case, termination of the business relationship or failure to provide service will be ensured by the AMLRO. It shall take all necessary steps without undue delay to ensure that the business relationship is effectively and legally terminated. In addition, it will prevent the client from being provided with any new services until the business relationship is terminated. (5) Furthermore, great care must be taken when assessing whether the client's conduct is showing signs of a suspicious transaction.

The following risk factors relate to the type E risk profile:

(a) there is a reasonable suspicion that the purpose of the business relationship is to provide services to a person other than himself (i.e., the client acts only as an intermediary or identity provider) and the client does not refute the suspicion;

(b) the client or a person associated with it (a member of the statutory body, beneficial owner, etc.) or another payment recipient (if known) is a person against whom the Republic of Bulgaria applies international sanctions;

(c) information provided by the client about himself / herself and his / her activities are grossly contrary to the reality, which was found from credible sources and the client did not justify the non-compliance;

(d) there is a reasonable suspicion that the client is providing false, misrepresented or incomplete information in the course of duration of the business relationship or that he is submitting false or altered documents;

(e) business relationship with this client has been terminated in the past due to the initiative of the Company;

(f) the client or a person associated with it (a member of the statutory body, the beneficial owner, etc.) is connected with another client with whom the business relation was terminated in the past due to the initiative of the Company;

(g) for other reasons, the client represents a significant risk to the Company in terms of money laundering or terrorism financing

(h) any of the factors listed above, if it occurs with a legal entity in which the client has a direct or indirect participation, or otherwise has the ability to exercise influence over it.

9. EXPANSION OF PEP RISK STATUS

For clients classified as PEPs, the following enhanced due diligence measures must be applied:

- **Risk Assessment**: A thorough risk assessment must be conducted to determine the potential risk of money laundering or financing of terrorism.

- **Source of Wealth**: The client must provide detailed information regarding the source of their wealth and the source of funds used in the business relationship.
- **Ongoing Monitoring**: All transactions conducted by a PEP client must be subject to enhanced and continuous monitoring to detect suspicious activity.
- **Approval from Senior Management**: Establishment or continuation of business relationships with a PEP must receive approval from senior management.

PEPs are excluded from any simplified customer due diligence processes. Simplified identification procedures may only be applied to clients with a low-risk profile (Type A), and therefore PEPs must undergo the full AML process, which includes:

- Comprehensive identification and verification procedures.
- Collection of additional information on the purpose and nature of the business relationship.

A person's status as a PEP remains for a minimum of 12 months following the cessation of their public duties. During this period, the individual is still considered to pose a higher risk, and enhanced due diligence must continue to be applied. After the 12-month period, a reassessment may be conducted to determine whether the individual's status can be revised.

All findings related to PEPs, including risk assessments, identification, and due diligence documentation, must be kept in the client's file for a minimum of 5 years after the termination of the business relationship. If any suspicious activity or red flags are identified during the course of the relationship, these must be immediately reported to the relevant authorities, in accordance with the local regulations.

The responsible person will update the identification data, information on whether or not the client is a PEP, whether the Republic of Bulgaria applies international sanctions against him or his related persons whenever the Company gets to know about any change and at least once in the following time intervals:

(a) every 12 calendar months for a client with a risk profile of the type A

(b) every 9 calendar months for a client with a risk profile of the type B,

(c) every 6 calendar months for a client with a risk profile of the type C and D.

The update is done by searching for identification and other data in public trusted sources or by asking the client if the identification and other data (PEP flag) are still current. In the case of a client with a risk profile of type B, C or D, it is not always sufficient within the framework of the update to provide written confirmation of the timeliness of the identification data, which Company keeps about the client.

10. INTERNATIONAL SANCTION SCREENING

The Company is committed to complying with all applicable international sanctions regulations, including those imposed by the United Nations, the European Union, the United States, and other relevant authorities. The Company will conduct sanctions screening on all potential clients, existing clients, and transactions against relevant sanction lists. This includes:

- **Screening of Clients**: All clients, both during onboarding and at regular intervals throughout the business relationship, will be screened against updated sanctions lists.
- **Screening of Transactions**: All transactions conducted by the Company, including payments, transfers, and any other financial activity, will be screened against sanctions lists prior to processing.
- **Third-party Relationships**: The Company will also screen third-party entities or intermediaries involved in the transaction process to ensure that they are not subject to sanctions.

The Company will ensure that sanctions screening is conducted against, but not limited to, the following major sanctions lists:

- United Nations (UN) Sanctions List
- European Union (EU) Sanctions List
- U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) List
- Her Majesty’s Treasury (HM Treasury) Consolidated List
- Other National and International Sanctions Lists: Any other sanctions lists applicable to the jurisdictions in which the Company operates.

The Company adopts a risk-based approach in its screening process:

High-Risk Clients: Clients who are considered high-risk, including Politically Exposed Persons (PEPs) or clients from high-risk jurisdictions, will undergo additional due diligence and monitoring.

Screening Frequency: New clients will be screened during onboarding, and existing clients will be re-screened on a regular basis, at least annually or whenever there is a significant update to the sanctions lists.

Sanctioned Country Screening: In addition to screening individuals and entities, the Company will also review transactions involving countries that are subject to comprehensive sanctions or restrictive measures.

The responsible person is obliged to create a record on the verification of international sanctions and on the result, which, i.e., contains at least the following information:

(1) date of verification and name of the person who performed the verification (whether performed by a specific responsible person or automated);

(2) a list of natural and legal persons that have been checked in the sanction lists;

(3) information on the sanction lists under which the verification was carried out;

(4) result of verification (negative or positive finding).

If a match or potential match is identified between a client, transaction, or third party and a person or entity on a sanctions list, the following steps will be taken:

- **Investigation**: The Compliance Department will investigate the match to determine whether it is a true match or a false positive. This may include additional research to confirm the identity of the individual or entity.
- **Immediate Action**: If a true match is identified, the transaction or business relationship will be immediately blocked or terminated, as required by applicable sanctions laws.
- **Reporting**: Any identified or suspected violations of sanctions will be reported to the relevant authorities in accordance with local and international regulatory requirements.

The Company will maintain records of all sanctions screenings, including the details of matches, actions taken, and communications related to the screening process. These records will be retained for a minimum of five years, or as required by applicable local regulations. Documentation will include:

- Copies of screening reports and matches.
- Details of investigations and actions taken following a match.
- Communications with relevant authorities.

11.INTERNAL SYSTEM OF POSITIONS FOR AML POLICY IMPLEMENTATION

Chief Executive Officer (CEO): Provide overall leadership and strategic direction for the Company. Ensure that the AML policy is integrated into the Company's operations and culture. The CEO is ultimately accountable for compliance with AML regulations and must foster a culture of compliance throughout the organization.

AMLRO: Oversee the implementation and adherence to AML policies and procedures. Ensure compliance with the AML Act and relevant EU directives. Develop and implement training programs for all responsible persons on AML policies, KYC procedures, and reporting obligations. Ensure ongoing education regarding updates in legislation and best practices. Conduct regular audits of AML compliance measures, assess the effectiveness of the AML program, and

recommend improvements. Ensure that documentation related to customer identification and transaction records is maintained accurately.

Customer Due Diligence (CDD) Team: Conduct risk assessments and perform customer verification processes. Ensure that Know Your Customer (KYC) procedures are followed for all clients.

Transaction Monitoring Team: Monitor transactions for suspicious activities and patterns indicative of money laundering or terrorist financing. Report any suspicious transactions to the Financial Intelligence Directorate.

Risk Management Officer: Identify, assess, and mitigate risks related to money laundering and terrorist financing. Collaborate with other teams to ensure a comprehensive approach to risk management.

12. DISTRIBUTION OF RESPONSIBILITY FOR AML/CTF MEASURES

Chief Executive Officer (CEO): The CEO holds ultimate responsibility for the overall compliance with AML/CTF laws and for ensuring the effective implementation of AML policies and procedures across all branches. The CEO shall provide leadership, allocate resources, and ensure that all branches adhere to national and international AML/CTF requirements.

Branch Managers: Each branch manager shall be responsible for the implementation of AML/CTF measures within their respective branch, ensuring that local procedures comply with the crypto-exchanger's central policies. Branch managers must also ensure that all staff members receive necessary training and that suspicious activities are reported promptly to the designated compliance officer.

AMLRO: The Compliance Officer oversees the coordination and execution of the AML/CTF program across all branches. This individual ensures that compliance measures are uniform and effective, conducts regular audits, and reports any deficiencies or issues directly to the CEO.

Other contractors/staff Members: All responsible persons across branches are responsible for adhering to the established AML/CTF procedures, including conducting customer due diligence (CDD), monitoring transactions, and reporting suspicious activities as outlined in the crypto-exchanger's policies.

Internal Audit and Monitoring: The internal audit function shall periodically assess the effectiveness of AML/CTF measures across all branches, ensuring consistency in compliance and identifying areas for improvement. The audit results will be reported to senior management, including the CEO, for review and necessary action.

13. PROCEDURES FOR VERIFICATION OF PROFESSIONAL COMPETENCE AND RELIABILITY IN HIRING AND ONGOING EVALUATION OF RESPONSIBLE PERSONS

All staff engaged in AML compliance must undergo a detailed background check, including criminal record verification, and must demonstrate expertise in AML laws, regulations, and risk management. New hires must complete comprehensive training on AML laws, crypto-specific risks, and the Company's AML policies. Periodic refresher courses are mandatory for all personnel. Responsible persons must regularly attend professional development programs to stay up-to-date with changes in legislation and emerging financial crime typologies. A performance evaluation system should be in place to ensure adherence to AML duties.

Before engaging in any transaction, all clients must undergo a risk-based CDD process, including identity verification and source of funds checks. Enhanced due diligence is required for high-risk clients. Crypto-exchange transactions and customer activity must be continuously monitored for unusual or suspicious behavior, and relevant reports must be submitted to the Financial Intelligence Unit (FIU). Any suspicious transaction, including potentially illicit transactions or money laundering, must be promptly reported to the FIU. Reports should be thoroughly documented, with a clear rationale and supporting evidence.

The Company should regularly perform internal audits and risk assessments to evaluate the effectiveness of compliance controls. Any breaches or lapses in AML procedures must be addressed promptly, and corrective actions should be implemented to prevent recurrence. The Company must maintain detailed records of all AML-related activities, including client identification, transaction monitoring, and suspicious activity reports, for at least five years as required by Bulgarian legislation. Regular reports on the operation of the AML service, its findings, and any suspicious activity should be submitted to the Company's senior management and relevant regulatory authorities.

14. RULES, POLICIES, AND PROCEDURES FOR CHECKING PROFESSIONAL COMPETENCE AND RELIABILITY OF RESPONSIBLE PERSONS UNDER AML POLICY

Candidates for roles with responsibilities related to AML must be thoroughly assessed for relevant knowledge, skills, and experience in AML, financial crime prevention, and cryptocurrency-specific risks. As part of the hiring process, all responsible persons must undergo a comprehensive background check, including:

Criminal Record: For Bulgarian citizens, a criminal record check is mandatory. For non-Bulgarian citizens, a similar document from their country of origin or residence must be provided to ensure no involvement in criminal activities related to financial crimes.

Other Documentation: Non-Bulgarian responsible persons may also be required to submit any other relevant documents, such as proof of professional qualifications or references from previous employers in the field of AML or related areas.

Responsible persons with AML responsibilities should be regularly evaluated through formal performance reviews to assess their competence, adherence to policies, and ability to identify and mitigate AML/TF risks.

Ongoing Competence: Responsible persons are required to undergo periodic assessments and audits of their AML-related activities to ensure they continue to meet professional standards and remain in compliance with legal obligations.

All responsible persons involved in AML-related duties must undergo a comprehensive onboarding training program that includes:

AML laws and regulations, particularly Bulgarian AML legislation.

Customer due diligence (CDD) procedures, including enhanced due diligence (EDD) for high-risk clients.

Identifying and reporting suspicious activities related to money laundering and terrorist financing.

Responsible persons must participate in ongoing training programs to stay updated on:

Changes in AML/TF regulations and guidelines.

Emerging risks and typologies in the cryptocurrency industry.

Internal updates on the crypto-exchanger's policies and procedures.

Responsible persons handling sensitive AML functions, such as transaction monitoring or SAR filing, must receive additional, specialized training related to risk assessment and reporting.

All background check documentation, including criminal records or similar documents for non-Bulgarian responsible persons, must be securely stored and accessible for review by relevant authorities.: Detailed records of all training activities, including responsible person attendance and completion, must be maintained for audit purposes.

Any failure to meet the competence or reliability standards set by the crypto-exchanger's AML policies should result in corrective action, including additional training or disciplinary measures. If an responsible person is found to have committed an act of financial crime, has a criminal record,

or fails to comply with AML procedures, immediate actions, including possible termination, should be considered.

15. COMPLIANCE OFFICER/ANTI MONEY LAUNDERING REPORTING OFFICER (AMLRO)

The AMLRO, is responsible for developing and maintaining appropriate anti-money laundering procedures and for receiving, considering and reporting, as appropriate, on any disclosure of suspicious activities by staff. The AMLRO or their delegation will investigate all reports or disclosures in accordance with the procedure.

The AMLRO is appointed by the Company's management and is responsible for developing, implementing, and monitoring the AML policy. Compliance management arrangements should include the appointment of a compliance officer at the management level.

The law mandates that institutions subject to AML/CTF obligations must appoint an MLRO. This officer is responsible for overseeing the organization's compliance with AML/CTF laws, reporting suspicious transactions, and ensuring that the institution's responsible persons are adequately trained in AML/CTF protocols.

Duties of the AMLRO:

1. Compliance Monitoring: The AMLRO must ensure that the institution’s AML/CTF policies are up-to-date and in compliance with current legislation.

2. Suspicious Transaction Reporting: The AMLRO is responsible for the timely reporting of suspicious activities to the Financial Analytical Office (FAÚ), the Republic of Bulgaria financial intelligence unit.

3. Internal Controls: The AMLRO is charged with developing and maintaining internal procedures for AML/CTF, including customer due diligence, record-keeping, and ongoing monitoring of customer activities.

4. Training and Awareness: The AMLRO must implement regular training programs to ensure that all responsible persons are aware of their AML/CTF responsibilities and can identify and report suspicious activities.

5. Communication with Authorities: The AMLRO serves as the main point of contact between the institution and regulatory authorities, particularly in matters related to AML/CTF compliance.

6. Risk Assessment: The AMLRO is tasked with conducting regular risk assessments to identify potential vulnerabilities in the institution’s AML/CTF defenses and taking necessary measures to mitigate these risks.

16. REPORTING BY THE AMLRO

The AMLRO reports directly to the top management, ensuring their independence in performing their duties. They have the authority to request any necessary information from responsible persons and conduct independent investigations under the AML policy.

These reporting duties include:

1. **Unusual Activity Report (UAR)**: The AMLRO is required to report any unusual transactions that may indicate money laundering or terrorism financing activities. These reports must be submitted to the Financial Analytical Office (FAO) without delay once a suspicion arises.

2. **Terrorist Property Reports (TPRs)**: In cases where transactions or activities involve assets suspected to be linked to terrorism, the AMLRO is obligated to file a report specifically focusing on terrorist property. These reports must highlight the nature of the suspicious activity and the connection to terrorist financing.

3. **Significant Transaction Reports (STRs)**: The AMLRO is responsible for identifying and reporting significant transactions that deviate from the customer's usual behavior, particularly those that appear suspicious due to their size, complexity, or pattern.

4. **Politically Exposed Persons (PEPs) Reports**: Transactions involving PEPs are subject to enhanced scrutiny. The AMLRO must report any unusual or suspicious activities linked to PEPs, given their increased risk of involvement in corruption and money laundering.

These obligations ensure that the financial institution complies with national and international standards in preventing money laundering and terrorist financing, while also maintaining transparency and accountability within its operations.

Unusual Activity Report

The AMLRO must identify and report any unusual activities that may indicate money laundering. Reports are prepared and submitted following internal procedures and legal requirements.

The AMLRO is responsible for completing and submitting the UAR, which must include:

- Subject/account holder identity
- Details and summary of the unusual activity/transaction
- A description and explanation of the activity
- Reporting officer or authorized individual details
- AMLRO’s declaration statement

Significant Transaction Reports (STR)

Any transactions exceeding a certain threshold or having unusual characteristics must be recorded and analyzed by the AMLRO for further action.

A Suspicious Transaction Report is a mandatory procedure for financial institutions when they detect transactions that may be linked to money laundering or terrorist financing. The process of reporting suspicious transactions is governed by the following key points:

Reporting Obligation:

- If obligated entities detect suspicious transactions, they are required to notify the authorities without undue delay. In cases of high risk of delay, the report must be made immediately after the suspicious transaction is discovered.
- If a full or partial investigation cannot be conducted, the obligated entity must submit a report on the suspicious transaction to the authorities.

Contents of the Report:

- The report must include the identification details of the person or account involved, details of all transaction participants known at the time of reporting, substantial circumstances of the transaction, and any other relevant information that might assist in assessing the case in terms of anti-money laundering or counter-terrorism financing measures.

Confidentiality:

- The report should not include information about the responsible person who discovered the suspicious transaction, except for their primary employment relationship.

Receipt of Reports:

- Authorities will receive reports on suspicious transactions. Information on how to submit reports, including remote access options, will be published by the authorities.

International Sanctions:

- If the suspicious transaction involves property subject to international sanctions aimed at maintaining or restoring international peace and security, protecting fundamental human rights, or combating terrorism, this must be noted in the report. The report should also include a brief description of the property, its

location, and owner if known, as well as information about any immediate risk of damage, deterioration, or illegal use of the property.

Contact Information:

- Simultaneously with the report, the obligated entity must provide the name, surname, and position of the contact person or the individual who processed the report, along with their contact details.

Failure to Conduct Due Diligence:

- If the report relates to a failure to conduct client due diligence, the obligated entity must detail the circumstances and reasons for the failure or partial failure of the due diligence process, and specify which particular procedures were not completed.

Joint Reporting:

- If multiple obligated entities jointly discover a suspicious transaction through information exchange, all involved entities are responsible for reporting the suspicious transaction. The report should indicate which other entities are also involved.

Reporting a suspicious transaction does not breach confidentiality obligations and should not subject responsible persons or individuals acting on behalf of the obligated entity to adverse actions. They should not face measures that could be reasonably considered as interference with their rights or legitimate interests due to the reporting of the suspicious transaction.

These provisions ensure effective detection and reporting of suspicious transactions, aiding in the fight against financial crimes and protecting the rights and interests of all parties involved.

Politically Exposed Person's Reports (PEP)

The AMLRO is required to maintain a register of transactions involving politically exposed persons and conduct thorough checks on such transactions to mitigate risks.

Financial institutions should be required, in relation to foreign politically exposed persons (PEPs) (whether as customers or beneficial owners), to undertake the following additional measures beyond normal customer due diligence:

(a) Implement Risk Management Systems: Develop and maintain appropriate systems to determine if a customer or beneficial owner is a politically exposed person.

(b) Obtain Senior Management Approval: Secure approval from senior management before establishing or continuing business relationships with such individuals.

(c) Establish Source of Wealth and Funds: Take reasonable steps to verify the source of wealth and source of funds of the customer or beneficial owner.

(d) Conduct Enhanced Ongoing Monitoring: Apply enhanced ongoing monitoring to the business relationship.

Financial institutions should also be required to determine if a customer or beneficial owner is a domestic PEP or someone who is or has been entrusted with a prominent function by an international organization. For higher-risk business relationships with such individuals, financial institutions should apply the measures outlined in (b), (c), and (d).

The same requirements for all types of PEPs should also apply to their family members or close associates.

17. UPDATE OF INFORMATION. THE TIME INTERVALS DURING WHICH THE MAINTAINED DATABASES AND CUSTOMER FILES ARE REVIEWED

The responsible person shall update the information concerning the purpose of the business relationship and risk profile: (a) every 12 calendar months for a client with a risk profile of the type A (b) every 9 calendar months for a client with a risk profile of the type B, (c) every 6 calendar months for a client with a risk profile of the type C and D. In case of change of the information concerning the purpose of the business relationship, or in case of the changes in ownership and management structure. Clients with the risk profiles B, C or D are obliged to prove the mentioned structure up to UBOs.

Every 6 months, the responsible person checks:

(a) for a client with risk profile of the type A – of other 3 randomly selected transaction of any volume. The responsible person may also request additional proof of economic activity in the form of 2 invoices from the suppliers.

(b) for a client with risk profile of the type B – of 5 other randomly selected transaction of any volume. An responsible person may also request additional proof of economic activity in the form of 2 invoices from the suppliers.

(c) for a client with risk profile of the type C – and of 10 other randomly selected transaction of any volume. An responsible person may also request additional proof of economic activity in the form of 4 invoices from the suppliers and 4 actual contracts.

(a) for a client with risk profile of the type D – of 20 transactions exceeding 15 000 EUR and of other 20 randomly selected transactions of any volume. An responsible person may also request

additional proof of economic activity in the form of 4 invoices from the suppliers and 4 actual contracts.

Business control of the client is focused on comparison of the real business activity of the client to the one that was declared. It is performed if the expected amount and volume of transactions is exceeded by 50%. The client is supposed to provide confirmation about his income and business activity and new limits should be set.

In case the criteria for the mentioned business control were met, it is necessary to ask the client to submit confirmation of income and business activity (in case of using services for business purposes). Once the business control happened, the new limits should be set for funds.

If a client has been assigned a risk profile of the type D, the client's source of funds must be verified from an independent source, not simply relying on the client's oral or written statement (i.e., accounting documents, third party documents, audited documents, etc.); the responsible person shall make and keep a copy of such a document (a standard copy is sufficient to be kept) or keep the original of the document; otherwise the responsible person will not execute the transaction with all the consequences (the client is obliged to comply with such a request and if he refuses, it is a suspicious transaction that must be reported).

18. COLLECTING, STORING, AND DISCLOSING INFORMATION

Customer information is collected to comply with AML regulations. The Company will collect personal data such as: full legal name, date of birth, address (proof of residence), identification documents (e.g., passport or national ID), source of funds declaration etc.

The Company can also additionally pledge logistical and technical means of customer verification. In case of non-verification, provision of false data by the client or refusal to provide data, the Company may refuse the transaction and report the suspicious transaction to the relevant authorities

All collected information will be stored securely using industry-standard encryption methods to protect against unauthorized access and data breaches.

Customer data will be retained for a minimum of five years after the termination of the business relationship, in compliance with AML regulations.

Access to personal data will be restricted to authorized personnel only, including compliance officers and designated staff responsible for AML monitoring.

The Company may disclose customer information to regulatory authorities, such as the Financial Intelligence Directorate, as required by law for AML compliance. Customer information will not be shared with third parties without prior consent, except in cases where disclosure is mandated by law or necessary for fraud prevention and investigation. In the event of a data breach that

compromises customer information, affected customers will be notified promptly in accordance with applicable data protection laws.

19. PROCEDURE FOR ANONYMOUS AND INDEPENDENT SUBMISSION OF INTERNAL REPORTS

The crypto-exchanger provides a secure and confidential reporting mechanism that allows responsible persons and other stakeholders to submit reports of violations, suspicious activities, or compliance issues anonymously.

The organization will conduct regular training sessions to inform responsible persons about:

The importance of reporting suspicious activities.

Procedures for submitting reports.

Rights and protections under this policy.

Available reporting channels include a confidential email address specifically designated for receiving reports and A secure physical drop box located in a designated area of the workplace.

Reports must be submitted directly to the designated independent internal unit, such as the AML department or a compliance officer, to ensure that the reporting process remains impartial and free from external influence or conflict of interest.

Responsible persons are required to report, even if the suspicion is not fully verified, any of the following:

- Suspicious activity that may involve money laundering or terrorist financing.
- Violations of the AML Act, the LMFT, or other related regulations, either by the Company or by individual responsible persons.

Reports should include the following information, if available:

- Description of the suspicious activity, including parties involved, transactions, and relevant dates.
- The reasons for suspicion, supported by any available evidence or documentation.
- The identity of the reporter, unless the report is submitted anonymously.

Reports will be investigated promptly and thoroughly, ensuring that the identity of the reporter remains confidential throughout the investigation process.

All reports, including anonymous submissions, will be handled confidentially to protect the identity of the reporter. The contents of the report will be kept strictly confidential to the extent possible.

The crypto-exchanger is committed to protecting responsible persons who submit reports in good faith from any form of retaliation. This includes protection from dismissal, demotion, harassment, or discrimination. Responsible persons who report violations or suspicions will not be penalized for their actions.

The organization is committed to protecting individuals who report suspicions in good faith from retaliation. This includes: assurance that no disciplinary action will be taken against whistleblowers, regardless of the outcome of any investigation. Clear consequences for any responsible person who retaliates against a whistleblower.

All reports will be reviewed by the designated AMLRO or head of the specialized service. If the report concerns a credible violation of AML or TF laws, an internal investigation will be initiated promptly.

If the internal investigation reveals a potential violation of the law, the matter will be escalated to senior management and, if necessary, reported to the Bulgarian Financial Intelligence Unit (FIU) or relevant law enforcement authorities in accordance with legal requirements.

All responsible persons will be trained on the reporting procedure, including:

- Their right to report suspicions or violations confidentially and anonymously.
- How to use the anonymous reporting channels.
- The protections offered to whistleblowers under this policy.

The crypto-exchanger will maintain a confidential record of all reports submitted, including the actions taken and outcomes of any investigations. These records will be securely stored and kept for the required retention period in accordance with Bulgarian legal obligations.

20. RULES FOR DISTRIBUTION OF RESPONSIBILITY OF THE REPRESENTATIVES AND RESPONSIBLE PERSONS OF THE PERSON UNDER ART. 4, AS WELL AS TO PERSONS IN A SIMILAR SITUATION

The person designated under Art. 4 of the AML Act is primarily responsible for ensuring compliance with all obligations set out in the AML Act and the Law on Measures against the Financing of Terrorism. This includes overseeing the development, implementation, and maintenance of the AML program, ensuring staff are trained, and reporting suspicious activities to relevant authorities.

The head of the specialized service, in cooperation with the person under Art. 4, is responsible for the operational implementation of AML policies, performing customer due diligence (CDD), monitoring transactions, conducting internal audits, and ensuring compliance with all legal requirements.

Other Responsible persons and Representatives: All responsible persons, representatives, and individuals involved in the crypto-exchanger's operations who have access to financial data or customer accounts are responsible for:

Complying with internal AML policies and procedures.

Performing appropriate CDD on clients, especially in high-risk situations.

Reporting any suspicious activities that could be related to money laundering or terrorist financing.

External Partners/Contractors: Individuals or entities engaged on a contractual basis (such as IT service providers, auditors, etc.) who handle sensitive information or assist with AML processes are also responsible for ensuring compliance with applicable AML regulations and confidentiality agreements.

The designated responsible person (under Art. 4) and the head of the AML service must ensure that all AML obligations are fulfilled, including:

Conducting customer due diligence.

Monitoring and reporting suspicious transactions.

Maintaining records as required by Bulgarian law.

All relevant staff must undergo initial and ongoing training regarding AML laws, risk management, and internal reporting procedures.

The responsible persons and departments must cooperate fully with the Bulgarian Financial Intelligence Unit (FIU) and other regulatory bodies, submitting required reports and ensuring transparency in AML efforts.

To ensure effective communication and compliance with the requirements of the AML Act and the Law on Measures against the Financing of Terrorism, the following contact details must be provided for the designated responsible person and the key responsible persons engaged in AML activities:

Person under Art. 4 - Person Responsible for overall compliance, Head of the Specialized Service (AMLRO), AML Compliance Team, Additional Representatives (e.g., external auditors, contractors):

Name:

Position:

Contact Information (Phone, Email, Office Address):

Contact details and records of the distribution of responsibilities for AML compliance must be maintained and updated regularly.

These records should be accessible for inspection by relevant authorities as needed.

21. APPLICATION OF THIS POLICY. POLICY REVIEW AND UPDATES

This Policy applies to all persons, including those working with Company on a purely voluntary basis. Company will terminate its involvement with any persons or entity who fail to comply with this Policy.

The AML policy will be reviewed and updated on a regular basis to ensure its ongoing relevance, effectiveness, and alignment with evolving legal and regulatory requirements. Reviews will be conducted annually, or more frequently if significant changes in legislation, regulatory guidance, or industry best practices occur. This process will include an evaluation of the current policy's performance, identification of areas for improvement, and the implementation of necessary adjustments to enhance the Company's AML framework. Any updates to the policy will be documented and communicated to all relevant staff members to ensure awareness and compliance across the organization.

The internal control procedures shall be reviewed at least annually to assess their effectiveness in preventing money laundering and terrorist financing, ensuring compliance with the latest regulatory changes. A designated team, led by the ALMRO, shall verify that all internal control mechanisms are in full compliance with the applicable laws, including ensuring proper implementation of customer due diligence, transaction monitoring, and suspicious activity reporting. Regular evaluations, including audits and risk assessments, shall be conducted to identify potential gaps or weaknesses in the internal control system. Adjustments shall be made based on findings to ensure continuous improvement. All review, verification, and evaluation processes shall be thoroughly documented, including the identification of any non-compliance issues, corrective actions taken, and improvements implemented. The results of the reviews and evaluations shall be reported to senior management to ensure oversight and ensure that necessary corrective actions are taken in a timely manner.

22.INDEPENDENT AUDIT

An independent audit shall be conducted if there are significant changes in the business operations, increased risk exposure, or as part of a regular review to ensure continued compliance with the AML Act and the Law on Measures Against the Financing of Terrorism. The audit shall assess the adequacy of internal controls, including customer due diligence, transaction monitoring, reporting of suspicious activities, and compliance with relevant AML/CTF regulations. The audit shall be carried out by an independent third-party auditor with expertise in AML/CTF compliance and no conflict of interest with the Company. The auditor shall provide a

comprehensive report to senior management, outlining the findings, identifying any weaknesses or non-compliance, and recommending corrective actions or improvements. Based on the audit findings, management shall ensure timely implementation of any corrective actions and improvements to maintain compliance with the relevant legislation.