ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING COMPLIANCE POLICY (GUIDELINES)

1. INTRODUCTION

This Anti-Money Laundering and Counter-Terrorist Financing Policy (the "Policy") establishes the framework for preventing, detecting, and mitigating risks related to money laundering, terrorist financing, and other financial crimes in connection with the services provided through the Application as further described in Section 4.3. (the "Services").

This Policy applies to all entities forming part of the Group, being the collective of affiliated entities involved in the provision, operation, and support of the Services.

Each entity within the Group operates in accordance with the laws and regulations applicable to it in its respective jurisdiction. The allocation of responsibilities between Group entities reflects their respective operational roles, while ensuring a consistent and coordinated approach to compliance across the Group.

The Group's AML/CTF framework is designed in accordance with internationally recognized standards and best practices, including but not limited to:

- the recommendations issued by the Financial Action Task Force (FATF), including the risk-based approach to AML/CTF compliance;
- the Basel AML Index and guidance from the Basel Institute on Governance;
- principles relating to customer due diligence and financial crime prevention issued by the Wolfsberg Group;
- applicable sanctions regimes issued by supranational bodies, including the United Nations, the European Union, and other relevant authorities;
- where applicable, regulatory guidance and expectations relating to crypto asset services issued by competent authorities in jurisdictions in which Group entities operate.

In addition to adhering to the above international standards, each entity within the Group complies with applicable Anti-Money Laundering, Counter-Terrorist Financing, and sanctions laws and regulations in the jurisdictions in which it is established and operates.

These Guidelines establish a unified AML/CTF framework applicable across the Group. Each Company implements and complies with these Guidelines to the extent required by its role, activities, and applicable legal and regulatory obligations.

The Group applies a risk-based approach to AML/CTF compliance, taking into account the nature, scale, and complexity of its operations, as well as the evolving risks associated with virtual assets and financial technologies.

The Group structure may evolve over time, and additional entities may participate in the provision of the Services. All such entities will be required to adhere to the principles and standards set out in this Policy. These Guidelines are subject to a review by the Management Board at least annually. Proposals for a review and the review of these Guidelines may be scheduled more frequently by the decision of theMoney Laundering Reporting Officer (MLRO) or the Compliance department or by other authorized persons.

2. DEFINITIONS

Beneficial Owner means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or exercises control in another manner over a transaction, act, action, operation or step or over another person and in whose interests or for whose benefit or on whose account a transaction or act, action, operation or step is made. In the case of a legal entity, the Beneficial Owner is a natural person whose direct or indirect holding, or the sum of all direct and indirect holdings in the legal entity, exceeds 25 percent, including holdings in the form of shares or other forms of bearer.

Business relationship shall mean a business, professional or commercial relationship between a customer and financial institutions or other obligated entities which is connected with their professional activities and which is expected, at the time when the contact is established, to have an element of duration.

Company or Companies means the relevant entity or entities within the Group that are responsible for the provision of the Services and/or for the implementation and oversight of AML/CTF obligations under this Policy, as determined by their respective roles and applicable legal requirements

Customer (Client, User) means a natural person or a legal entity which has the Business Relationship with the Company

Employee means the Company's employee and any other person who is involved in application of these Guidelines within the Group.

Group of Entities (Group) means the collective of current and/or future affiliated legal entities that may be involved in the provision, operation, or support of the Services, forming part of the same organizational and operational structure. For the avoidance of doubt, the Group does not include independent third-party service providers. Each entity within the Group operates in accordance with the laws and regulations applicable to it in its respective jurisdiction.

Guidelines – this document including inter alia the Group's internal control procedure regarding the Guidelines and the Group's risk assessment policy regarding risk-based approach for ML/TF risks.

Management Board shall be understood as references to the governing body of the relevant Group entity responsible for the provision of the Services, unless the context requires otherwise.

MLRO means Money Laundering Reporting Officer, who is appointed within the Group to perform money laundering reporting and AML/CTF compliance functions, whether at Group level or within a specific Group entity, as required by applicable laws

Monetary Operation means any payment, transfer or receipt of money.

Money Laundering (ML) means the concealment of the origins of illicit funds

through their introduction into the legal economic system and transactions that appear to be legitimate.

There are three recognized stages in the Money Laundering process:

- placement, which involves placing the proceeds of crime into the financial system;
- layering, which involves converting the proceeds of crime into another form and creating complex layers of financial transactions to disguise the audit trail and the source and ownership of funds;
- integration, which involves placing the laundered proceeds back into the economy to create the perception of legitimacy.

Politically Exposed Person (PEP) means a natural person who performs or has performed prominent public functions and with regard to whom related risks remain.

Sanctions mean an essential tool of foreign policy aimed at supporting the maintenance or restoration of peace, international security, democracy and the rule of law, following human rights and international law or achieving other objectives of the United Nations Charter or the common foreign and security Policy of the European Union as well as various international agreements, regulatory frameworks, resolutions of intergovernmental organizations, and decisions of relevant supervisory and enforcement bodies.

Sanctions include:

- international Sanctions which are imposed with regard to a state, territory, territorial unit, regime, organization, association, group or person by a resolution of the United Nations Security Council, a decision of the Council of the European Union or any other legislation issued in the jurisdiction the Group operates ;
- Sanctions imposed by competent governmental or regulatory authorities in any relevant jurisdiction, including those applicable based on the Company's place of incorporation, operation, licensing, or business activities.

International Sanctions may ban the entry of a subject of an international Sanction in the state, restrict international trade and international transactions, and impose other prohibitions or obligations.

The subject of Sanctions is any natural or legal person, entity, or body, designated in the legal act imposing or implementing Sanctions, with regard to which the Sanctions apply.

Terrorist Financing (TF) means the financing and supporting of an act of terrorism and commissioning thereof as well as the financing and supporting of travel for the purpose of terrorism in the meaning of applicable legislation.

Crypto-asset means a digital representation of value or rights that can be transferred and stored electronically using distributed ledger technology or similar technology.

Crypto-asset Address means address/account generated from letters, numbers

and/or symbols in the blockchain, by which the blockchain allocates the Crypto-asset to the owner or recipient.

3. PRINCIPLES FOR STRUCTURE AND MANAGEMENT OF THE COMPANY

The organizational structure of the Group must correspond to its size and the nature, scope, and level of complexity of its activities and services provided, including the risk appetite and related risks, and must be structured in accordance with the principle of three lines of defense. The organizational structure of the Group must correspond to the complete understanding of potential risks and their management. The reporting and subordination chains of the Group must be ensured in such a way that all Employees know their place in the organizational structure and know their work duties.

3.1. The Management Board

The Management Board is the carrier of the culture of compliance with the requirements of Money Laundering and Terrorist Financing prevention, guaranteeing that the Management Board members and Employees of the Company operate in an environment where they are fully aware of the requirements for the prevention of Money Laundering and Terrorist Financing and the obligations associated with these requirements, and the relevant risk considerations are taken into account to a suitable extent in the decision-making processes of the Company.

The Management Board members bear ultimate responsibility for the measures taken to prevent the use of the Company's services for Money Laundering or Terrorist Financing.

They provide oversight and are accountable for:

- establishing and maintaining AML processes, procedures, risk, and control processes;
- adopting these Guidelines and other internal guidelines and instructions;
- determining the Company's Guidelines for AML measures;
- appointing an MLRO and ensuring that the MLRO has the powers, resources and expertise required to perform their assignment;
- allocating sufficient resources to ensure the effective implementation of the Guidelines and other related documents and to maintain the organization;
- ensuring all relevant Employees complete annual AML training.

3.2. The first line of defense – the Employees

The first line of defense has the function of applying the due diligence measures upon Business Relationship and applying due diligence measures during the Business Relationship. First line of defense comprises the structural units and Employees of the Group with whose activities risks are associated and that must identify and assess these risks, their specific features and scope and that manage these risks by way of their ordinary activities, primarily by way of application of due diligence measures.

The risks arising from the activities of and provision of services by the Group belong to the first line of defense. They are the managers (owners) of these risks and responsible for them. The Employees of the Group must act with the foresight and competence expected from them and according to the requirements set for their positions, proceeding from the interests and the goals of the Group, and ensure that the Group's financial system and economic space are not used for Money Laundering and Terrorist Financing.

The Company takes measures to assess the suitability of the Employees before they start working with the relevant training. For the aforementioned reasons, the Employees are required to:

- adhere to all requirements outlined in the Guidelines and other related documents;
- collect required Customer information in accordance with their function and accountabilities;
- report information, situations, activities, transactions or attempted transactions that are unusual for any type of service or Customer relationship, regardless of the amount, whether or not the transaction was completed without delay to the MLRO;
- not inform or otherwise make Customers aware if the Customer or any other Customers are or may be the subject of a report or if a report has been or may be filed;
- complete the appropriate AML training required for the Employee's position.

3.3. The second line of defense – Risk Management and Compliance, MLRO

The second line of defense consists of the risk management and compliance functions. These functions may also be performed by the same person or structural unit depending on the size of the Group and the nature, scope and level of complexity of their activities and provided services, incl. the risk appetite and risks arising from activities of the Group..

The objective of the compliance function is to guarantee that the Group complies with effective legislation, guidelines and other documents and to assess the possible effect of any changes in the legal or regulatory environment on the activities of the Group and on the compliance framework.

The task of compliance is to help the first line of defense as the owners of risk to define the places where risks manifest themselves (e.g., analysis of suspicious and unusual transactions, for which compliance Employees have the required professional skills, personal qualities, etc.) and to help the first line of defense manage these risks efficiently. The second line of defense does not engage in taking risks.

The Group establishes and implements a separate Risk policy,in which the risk management framework is controlled by the Compliance department. The Compliance department ensures that all risks are identified, assessed, measured, monitored, and managed, and informs the appropriate units of the Company about them. The Development department provides risk management and business continuity functions and plays a

critical role in ensuring operational resilience and mitigating potential disruptions to business operations.

The Management Board has appointed a MLRO for performing the second line of defense functions. The Management Board is not operationally involved in the areas that the MLRO will be monitoring and verifying and is thus independent in relation to them.

The MLRO is responsible for the following activities:

- produce and, when necessary, update the Company's Guidelines;
- monitor and verify on an ongoing basis that the Company is fulfilling the requirements prescribed by these Guidelines and related documents and according to external laws and regulations;
- provide the Company's staff and members of the Management Board with advice and support regarding the rules relating to Money Laundering and Terrorist Financing;
- inform and train the members of the Management Board and relevant persons about the rules relating to Money Laundering and Terrorist Financing;
- investigate and register sufficient data on received internal notifications and decide whether the activity can be justified or whether it is suspicious;
- file the relevant reports with the appropriate regulatory authorities in accordance with applicable legislation;
- check and regularly assess whether the Group's procedures and guidelines to prevent the use of the business for Money Laundering or Terrorist Financing are fit for purpose and effective.
- ensuring the implementation of risk-based monitoring measures.
- maintaining internal reporting mechanisms for suspicious transactions.

The MLRO reports to the Management Board quarterly.This report must be in writing and include at least the following items:

- number of Customers under all risk classifications
- number of hits of persons in relation to the Sanctions lists and applied measures;
- number of Customers or Customers' representatives identified as PEPs or persons with a connection to a PEP;
- number of internal notifications on suspicious activity or transactions;
- number of the relevant reports reported to the supervisory authorities ;
- number and content of a request for information from the supervisory authorities within the framework of an investigation;
- confirmation that the Group's risk assessment for Money Laundering and Terrorist Financing is up to date;
- confirmation that these Guidelines and other related documents are up to date;
- confirmation that the staffing in respect of AML measures is sufficient;
- all inadequacies (if any) identified by control function have been addressed;
- list of obligatory trainings which have been held for the staff in respect of AML

measures.

3.4. The third line of defense – Internal Audit

The third line of defense is comprised by the independent and effective internal audit function. The internal audit function may be performed by one or several Employees, the Group's structural unit with the relevant functions or by the third party, which provides the relevant service to the Company.

The Employees, the Group's structural unit or third party, which performs the internal audit function must have the required competency, tools, and access to the relevant information in all structural units of the Group. The internal audit methods must comply with the size of the Group , the nature, scope, and level of complexity of the activities and provided services, incl. the risk appetite and risks arising from activities of the Group. .

The decision to conduct an internal audit is made by a resolution of the Management Board. The Management Board must assess the need to conduct an internal audit at least annually.

4. PRINCIPLES OF CUSTOMER DUE DILIGENCE MEASURES IMPLEMENTATION

Customer due diligence (CDD) measures are required for verifying the identity of a new or existing Customer as a well-performing risk-based ongoing monitoring of the Business Relationship with the Customer.

The CDD measures consist of 3 levels, including simplified and enhanced due diligence measures, as specified below.

4.1. Main Principles

The CDD measures are taken and performed to the extent necessary considering the Customer's risk profile and other circumstances in the following cases:

- upon establishment of the Business Relationship and during the ongoing monitoring of the Business Relationship;
- upon verification of information gathered while applying due diligence measures or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered earlier while updating the relevant data;
- upon suspicion of Money Laundering or Terrorist Financing, regardless of any derogations, exceptions or limits provided for in these Guidelines and applicable legislation.

The Company does not establish or maintain the Business Relationship and does not perform the transaction if:

- the Company is not able to take and perform any of required CDD measures;
- the Company has any suspicions that the Company's services or transaction will be used for Money Laundering or Terrorist Financing;

- the risk level of the Customer or of the transaction does not comply with the Group's risk appetite.

In the case of receiving information in foreign languages within the framework of CDD implementation, the Company may request the translation of the documents to another language applicable for the Company. The use of translations should be avoided in situations where the original documents are prepared in a language applicable for the Company.

Achieving CDD is a process that starts with the implementation of CDD measures. When that process is complete, the Customer is assigned a documented individual risk level which shall form the basis for follow-up measures, and which is followed up and updated when necessary.

The Company has applied CDD measures adequately if the Company has the inner conviction that they have complied with the obligation to apply due diligence measures. The principle of reasonability is observed in the consideration of inner conviction. This means that the Company must, upon the application of CDD measures, acquire the knowledge, understanding and assertion that they have collected enough information about the Customer, the Customer's activities, the purpose of the Business Relationship and of the transactions carried out within the scope of the Business Relationship, the origin of the funds, or any other related information, so that they understand the Customer and the Customer's (business) activities, thereby taking into account the Customer's risk level, the risk associated with the Business Relationship and the nature of such relationship.

Such a level of assertion must make it possible to identify complicated, high-value and unusual transactions and transaction patterns that have no reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

4.2. The Services Provided

The Services are made available through the Trustee Plus application.

The Services provided through the application include, without limitation:

- the provision of hosted wallet services enabling users to access, store, and manage crypto-assets;
- the deposit, transfer, and withdrawal of crypto-assets;
- the exchange of crypto-assets for fiat currency and vice versa;
- the exchange of crypto-assets for other crypto-assets; and

any other services involving crypto-assets that may be made available through the application from time to time.

The Company provides the aforementioned services including but not limited to crypto-assets : BTC, ETH, LTC, TRX and others.

4.3. The Verification of Information used for the Customer's Identification

Verification of the information for the Customer's identification means using data from a reliable and independent source to confirm that the data is true and correct, also confirming, if necessary, that the data directly related to the Customer is true and correct. This, inter alia, means that the purpose of verification of information is to obtain reassurance that the Customer, who wants to establish the Business Relationship is the person they claim to be.

The reliable and independent source (must exist cumulatively) is verification of the information obtained in the course of identification:

- which originates from two different sources;
- which has been issued by (identity documents) or received from a third party or a place that has no interest in or connections with the Customer or the Company,i.e. that is neutral (e.g. information obtained from the Internet is not such information, as it often originates from the Customer themselves
- the reliability and independence of which can be determined without objective obstacles and reliability and independence are also understandable to a third party not involved in the Business Relationship; and
- the data included in which or obtained via which are up to date and relevant and the Company can obtain reassurance about this (and reassurance can in certain cases also be obtained on the basis of the two previous clauses).

4.4. Application of Simplified Due Diligence Measures (level 1)

Simplified due diligence (SDD) measures are applied where the Customer's risk profile indicates low risk level of ML/TF.

When applying SDD measures, the Company must only obtain the following data of the Customer who is a natural person:

- name(s) and surname(s);
- official personal number;

or in case of the Customer, which is a legal entity, the following data:

- the name under which the legal entity is registered;
- legal form;
- legal entity identifier (LEI) or a registration number, if such number has been issued;
- registered and official office address;
- the Customer´s representative name(s), surname(s) and personal number or date of birth; and

ensure that the first payment be carried out through an account with a credit institution, where the credit institution is registered in EEA or in a Third Country which imposes requirements equivalent to those laid down in the relevant law and is supervised

by competent authorities for compliance with those requirements.

SDD measures may be carried out only where the ongoing monitoring of the Customer's Business Relationship is performed in accordance with the Guidelines and there is a possibility to identify suspicious Monetary Operations and transactions. SDD measures must not be carried out in the circumstances where enhanced due diligence measures (as described below) must be carried out.

Where, in the course of performing ongoing monitoring of the Customer's Business Relationships, it is established that the risk of ML and/or TF is no longer low, the Company must apply the relevant level of CDD measures.

4.5. Application of Standard Due Diligence Measures (level 2)

Standard due diligence measures are applied to all Customers where CDD measures must be applied in accordance with the Guidelines. The following standard due diligence measures should be applied:

- identification of the Customer and verification of the submitted information based on information obtained from a reliable and independent source;
- identification and verification of a representative of the Customer and their right of representation;
- identification of the Beneficial Owner and, for the purpose of verifying their identity, taking measures to the extent that allows the Company to make certain that it knows who the Beneficial Owner is, and understands the ownership and control structure of the Customer;
- understanding of Business Relationship, transaction or operation and, where relevant, gathering information thereon;
- gathering information on whether the Customer is PEP, their family member or a person known to be close associate;
- monitoring of the Business Relationship.

The CDD measures specified above must be applied before establishing the Business Relationship or performing transaction. The exact instruction for application standard due diligence measures is provided in the Guidelines.

4.6. Application of Enhanced Due Diligence Measures (level 3)

In addition to standard due diligence measures, the Company applies enhanced due diligence (EDD) measures in order to manage and mitigate an established risk of Money Laundering and Terrorist Financing in the case where the risk is established to be higher than usual.

The Company always applies EDD measures, when:

- the Customer's risk profile indicates high risk level of ML / TF;
- upon identification of the Customer or verification of submitted information, there

are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the Beneficial Owner;

- where cross-border correspondent relationships are commenced with the Customer, which is financial institution of Third Country;
- in the case of performance of transaction or Business Relationship with the PEP, the family member of the PEP or a person known to be the close associate of the PEP;
- where transaction or Business Relationship is carried out with natural persons residing or legal persons established in high-risk Third Countries as identified by the European Commission or by the Internal Policies of the Company;
- the Customer is from such country or territory or their place of residence or seat or the seat of the payment service provider of the payee is in a country or territory that, according to credible sources such as mutual evaluations, reports or published follow-up reports, has not established effective AML/CFT systems that are in accordance with the recommendations of the FATF.
- where transfers including transfers of crypto-assets to or from a self-hosted address are taking place, as long as there is a crypto-asset service provider involved.
- where the Company encounters unusual or suspicious patterns of transactions or situations of higher risks of money laundering and terrorist financing associated with transfers involving self-hosted addresses

Prior to applying EDD measures, the Company's Employee ensures that the Business Relationship or transaction has a high risk and that a high-risk rate can be attributed to such Business Relationship or transaction. Above all, the Employee assesses prior to applying the EDD measures whether the features described above are present and applies them as independent grounds (that is, each of the factors identified allows application of EDD measures with respect to the Customer).

When applying EDD measures where cross-border correspondent relationship is commenced with the Customer, which is financial institution of Third Country, the Company must apply the following measures:

- gather sufficient information about the Customer to fully understand the nature of its business and to determine from publicly available information the reputation of the Customer and the quality of supervision;
- assess AML control mechanisms of the Customer and the entity receiving funds;
- obtain approval from the Management Board member before establishing new correspondent relationships;
- document the respective responsibilities of the Customer;
- be satisfied that the Customer has carried out proper Customer due diligence (including verification of the identity of the Customers having direct access to accounts of the Customer and performance of other Customer due diligence actions) and that it is able to provide the relevant Customer identification data to the Company upon its request.

When applying EDD measures, where transactions or Business Relationships are

carried out with the PEP, the family member of the PEP or a person known to be the close associate of the PEP, the Company must apply the following measures:

- obtain approval from the Management Board member before establishing Business Relationship with such Customer or continuing the Business Relationship with the Customer when he or she becomes a PEP;
- take adequate measures to establish the source of wealth and source of funds that are involved in the Business Relationship or transaction;
- perform ongoing monitoring of the Business Relationship with the Customer by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

When applying EDD measures where transaction or Business Relationship are carried out with natural persons residing or legal persons established in high-risk Third Countries as identified by the European Commission or by the Internal Policies of the Company, the Company must apply the following measures:

- obtain additional information on the Customer and on their Beneficial Owner;
- obtain additional information on the intended nature of the Business Relationship;
- obtain information on the source of funds and source of wealth of the Customer and their Beneficial Owner;
- obtain information on the reasons for the intended or performed transactions;
- obtain the approval of the Management Board member for establishing Business Relationships with the Customer or continuing Business Relationships with them;
- perform ongoing monitoring of the Business Relationship with the Customer by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;
- ensure that the first payment be carried out through an account in the Customer's name with a credit institution, where the credit institution is registered in a country which imposes requirements equivalent to those laid down in the applicable law and is supervised by competent authorities for compliance with those requirements.

When applying EDD measures where the Customer is from such country or territory or their place of residence or seat or the seat of the payment service provider of the payee is in a country or territory that, according to credible sources such as mutual evaluations, reports or published follow-up reports, has not established effective AML/CFT systems that are in accordance with the recommendations of the FATF, the Company must apply the following measures:

- obtain the approval of the Management Board member for establishing Business Relationships with the Customer or continuing Business Relationships with them;
- obtain information on the source of funds and source of wealth of the Customer and their Beneficial Owner;
- perform ongoing monitoring of the Business Relationship with the Customer by increasing the number and timing of controls applied, and selecting patterns of

transactions that need further examination;

In any other cases when EDD measures must be applied, the amount of EDD measures and the scope shall be determined by the Employee, who is applying such measures.

The following additional and relevant due diligence measures may be followed:

- verification of information additionally submitted upon identification of the Customer based on additional documents, data or information originating from a credible and independent source;
- gathering additional information on the purpose and nature of the Business Relationship or transaction and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;
- gathering additional information and documents regarding the actual execution of transactions made in the Business Relationship in order to rule out the ostensibility of the transactions;
- gathering additional information and documents for the purpose of identifying the source and origin of the funds used in a transaction made in the Business Relationship in order to rule out the ostensibility of the transactions;
- the making of the first payment related to a transaction via an account that has been opened in the name of the Customer participating in the transaction with a credit institution or financial institution that is subject to anti-money laundering and counter-terrorist financing requirements consistent with internationally recognized standards, including those established by the Financial Action Task Force;
- gathering additional information about the Customer and its Beneficial Owner, including identification of all owners of the Customer, incl. those whose shareholding is below 25%;
- gathering information on the origin of the funds and wealth of the Customer and its Beneficial Owner;
- improving the monitoring of the Business Relationship by increasing the number and frequency of the applied control measures and by choosing transaction indicators or transaction patterns that are additionally verified;
- obtaining the approval of the Management Board member for performing transactions or establishing business relationship with new and existing Customers

The Employee shall notify about EDD measures applied within 2 working days after the start of applying of the EDD measures by sending relevant notification to the MLRO.

In the case of application of EDD measures, the Company reassesses the Customer's risk profile no later than every month.

Employees handling transaction monitoring receive regular AML/CFT training on identifying risk factors.

The Company collects and assesses information in relation to self-hosted wallets to ensure compliance with applicable anti-money laundering and counter-terrorist financing requirements and internationally recognized standards

For self-hosted wallet transactions exceeding EUR 1,000, the Company:

- Obtains and stores information on the wallet owner.
- Verifies whether the wallet is owned or controlled by its customer.

If the origin or destination of the funds cannot be determined, the transfer is subject to additional scrutiny or rejection.

The Company determines whether a transfer involving a self-hosted address amounts to or exceeds EUR 1 000:

- at the moment the transfer was ordered or initiated, where the Company acts on behalf of the originator; or
- at the time of the receipt, where the Company acts on behalf of the beneficiary.

In order to assess whether the self-hosted address is owned or controlled by the originator or beneficiary, respectively, the Company uses at least one of the following verification methods:

- automated or non-interactive verification methods, including technical checks demonstrating control over the wallet address;
- verification involving direct interaction with the Customer ;
- sending of a predefined amount (preferably the smallest denomination of a given crypto-asset), between the Company and the self-hosted wallet;
- requesting the customer to digitally sign a specific message into the account and wallet software with the key corresponding to that address;
- other suitable technical means as long as they allow for reliable and secure assessment and the Company is fully satisfied that it knows who owns or controls the address.

Where the Company is fully satisfied that the self-hosted address is owned or controlled by the customer, the Company documents this in its systems and may not need to re-apply the measures above to subsequent transactions from/to the same address (‘whitelisting’). The Company has controls in place to identify changes in the ML/TF risk of the self-hosted address and its ownership or controllership. Should the Company establish that the ML/TF risk of the self-hosted address has changed or that there are indications that its customer no longer owns or controls the self-hosted address, the Company removes this address from its whitelist.

5. CUSTOMER DUE DILIGENCE MEASURES

5.1. Identification of the Customer – natural person

The Company identifies the Customer who is a natural person and, where relevant, their representative and retains the following data on the Customer:

- full name and surname as they appear in the customer's identity document
- official personal number or alternatively date of birth
- citizenship (1);
- photograph;
- signature

The following valid identity documents which contain data specified above may be used as the basis for the identification of a natural person:

- an identity document or a residence permit, the acceptance of which is subject to the Company's availability of services in the relevant geographical area.

The Customer, who is a natural person, cannot use a representative in the course of business relationship with the Company.

5.2. Identification of the Customer – legal entity

The Company identifies the Customer which is a legal entity and their representative and retains the following data on the Customer:

- the name under which the legal entity is registered;
- legal form;
- legal entity identifier (LEI) or a registration number, if such number has been issued;
- full name and surname as they appear in the customer's identity document, official personal number (in the case of an foreigner – date of birth or where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification) and citizenship of the director(s) or member(s) of the Management Board or member(s) of another equivalent body, and their authorities in representing the Customer;
- an extract of registration and its date of issuance;
- registered and official office address.

The following documents issued by a competent authority or body not earlier than six months before their use may be implied for identification of the Customer:

- registry card of the relevant register; or
- registration certificate of the relevant register; or
- a document equivalent with the aforementioned documents or relevant documents of establishment of the Customer.

The Company verifies the correctness of the Customer's data specified above, using information originating from a credible and independent source for that purpose. Where the Company has access to the relevant register of legal entities, the submission of the documents specified above do not need to be demanded from the Customer.

The identity of legal entity and the right of legal entity's representation can be verified on the basis of a document specified above, which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.

The Company ensures that all crypto-asset transfers comply with applicable requirements relating to the transmission of information, including those derived from Recommendation 16 of the Financial Action Task Force, ensuring the transmission of the following information before processing transactions:

For the Originator (Sender):

- full name and surname as they appear in the customer's identity document
- Wallet address or unique transaction identifier
- Customer account number or other identifier
- official personal document number, and customer identification number or, alternatively, the date of birth
- legal entity identifier (LEI), or any equivalent official identifier (if applicable)

For the Beneficiary (Receiver):

- full name and surname as they appear in the customer's identity document
- official personal document number, and customer identification number or, alternatively, the date of birth
- Wallet address or unique transaction identifier
- legal entity identifier (LEI), or any equivalent official identifier (if applicable)

All transactions are reviewed to ensure they contain the mandatory identifying information before execution. If information is missing or incomplete, the transaction is rejected, suspended, or further investigated based on a risk-based approach.

5.3. The identification of the Customer's (legal entity's) representative and their right of representation

The representative of the Customer shall be identified as the Customer, who is a natural person in accordance with these Guidelines. The Company must also identify and verify the nature and scope of the right of representation of the Customer. The name, date of issue and name of issuer of the document that serves as a basis for the right of representation must be ascertained and retained, except in case, when the right of

representation was verified using information originating from the relevant register.

The Company must observe the conditions of the right of representation granted to the legal entity's representatives and provide services only within the scope of the right of representation.

The authorisation must comply with the applicable legal requirements of the relevant jurisdiction. Authorisations issued in a foreign jurisdiction shall be duly legalised or apostilled, where required. In case the right of representation of the Customer (legal person) is evident from the registry extract, Articles of Association or equivalent documents evidencing the identity of the Customer (legal person), a separate document of authorisation (e.g. a Power of Attorney) should not be required.

5.4. The identification of the Customer's (legal entity's) Beneficial Owner

The Company must identify the Beneficial Owner of the Customer and take measures to verify the identity of the Beneficial Owner to the extent that allows the Company to make sure that they know who the Beneficial Owner is.

The Company collects the following data regarding the Customer's Beneficial Owner(s):

- full name and surname as they appear in the customer's identity document;
- official personal number or, alternatively, the date of birth
- citizenship (2).

The Company shall request from the Customer information of the Customer's Beneficial Owner (e. g. providing the Customer with an opportunity to specify their Beneficial Owner when collecting data about the Customer).

The Company doesn't establish the Business Relationship, if the Customer, who is a natural person, has a Beneficial Owner who is not the same person as the Customer.

The Beneficial Owner of a legal entity is identified in stages where the obliged entity proceeds to each subsequent stage if the Beneficial Owner of the legal entity cannot be determined in the case of the previous stage.

The stages are as follows:

- is it possible to identify, in respect of the Customer that is a legal entity or a person participating in the transaction, the natural person or persons who actually ultimately control the legal entity or exercise influence or control over it in any other manner, irrespective of the size of the shares, voting rights or ownership rights or its direct or indirect nature;
- whether the Customer that is a legal entity or the person participating in the transaction has a natural person or persons who own or control the legal entity via direct (3) or indirect (4) shareholding. Family connections and contractual connections must also be taken into account here;

- who is the natural person in senior management (5), who must be defined as the Beneficial Owner, as a result of execution of the previous two stages have not made it possible for the obliged entity to identify the Beneficial Owner. The documents used for the legal entity´s identification or the other submitted documents do not indicate directly who the Beneficial Owner of the legal entity is, the relevant data (incl. data about being a member of a group and the ownership and management structure of the group) are registered on the basis of the statement of the representative of the legal entity or the document written by hand by the representative of the legal entity.

The Company shall apply reasonable measures to verify the accuracy of the information established on the basis of statements or a handwritten document (e.g. by making inquiries in the relevant registers), requiring the submission of the legal entity's annual report or other relevant document. If the Company has doubts about the accuracy or completeness of the relevant information, the Company shall verify the information provided from publicly available sources and, if necessary, request additional information from the Customer.

Where the Company establishes the Business Relationship with the Customer whose information on Beneficial Owners must, in accordance with the legislation of EEA´s state, be submitted to the state or be registered there, the Company shall obtain a relevant registration certificate or registry extract upon identification of the Customer´s Beneficial Owner.

5.6. Political Exposed Person's identification

The Company shall take measures to ascertain whether the Customer, the Beneficial Owner of the Customer or the representative of this Customer is a PEP, their family member (6) or close associate (7) or if the Customer has become such a person.

The Company shall request from the Customer information to identify if the Customer is a PEP, their family member or close associate (e. g. providing the Customer with an opportunity to specify the relevant information when collecting data about the Customer).

The Company shall verify the data received from the Customer by making inquiries in relevant databases or public databases or making inquiries or verifying data on the websites of the relevant supervisory authorities or institutions of the country in which the Customer has place of residence or seat.

PEP must be additionally verified using international search engine (e. g. Google) and the local search engine of the Customer's country of origin, if any, by entering the Customer's name in both Latin and local alphabet with the Customer's date of birth.

At least, but not limited to, the following persons are deemed to be PEPs:

- the head of the state, the head of the government, a minister, a vice- minister or a

deputy minister, a secretary of the state, a chancellor of the parliament, government or a ministry;

- a member of the parliament;
- a member of the Supreme Court, the Constitutional Court or any other supreme judicial authorities whose decisions are not subject to appeal;
- a mayor of the municipality, a head of the municipal administration;
- a member of the management body of the supreme institution of state audit or control, or a chair, deputy chair or a member of the board of the central bank;
- ambassadors of foreign states, a chargé d'affaires ad interim, the head of the armed forces, command of the armed forces and units, chief of defense staff or senior officer of foreign armed forces;
- a member of the management or supervisory body of a public undertaking, a public limited company or a private limited company, whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, are owned by the state;
- a member of the management, executive or supervisory body of a state-owned enterprise, a municipal undertaking, or a company in which the State Treasury or a local government unit holds, directly or indirectly, more than 50% of shares or voting rights, as well as persons holding public functions defined as politically exposed persons (PEPs) ;
- a director, a deputy director or a member of the management or supervisory body of an international intergovernmental organisation;
- a leader, a deputy leader or a member of the management body of a political party.

The Company shall identify close associates and family members of PEPs only if their connection with PEP is known to the public or if the Company has reason to believe that such a connection exists.

Where the Customer who is a PEP no longer performs important public functions placed upon them, the Company shall at least within 12 months take into account the risks that remain related to the Customer and apply relevant and risk sensitivity-based measures as long as it is certain that the risks characteristic of PEPs no longer exist in the case of the Customer.

5.7. Identification of the purpose and nature of the business relationship or a transaction

The Company shall understand the purpose and nature of the establishing Business Relationship or performing transaction. Regarding the services provided, the Company may request from the Customer the following information for understanding the purpose and nature of the Business Relationship or transaction:

- whether the Customer will use the services of the Company for their own needs or will represent the interests of another person;

- contact information;
- information on the registered address and actual living address of the Customer;
- the estimated transactions turnover with the Company per calendar year;
- the estimated source of funds used in the Business Relationship or transaction;
- if the Business Relationship or transaction is related to the Customer´s performance of economic or professional activities and which activities they are;
- information on the source of funds related to the Business Relationship or transaction, if amount of transactions (incl. expected amount) exceeds established limit.

The Company shall apply additional measures and collect additional information to identify the purpose and nature of the Business Relationship in cases where:

- there is a situation that refers to high value or is unusual and/or
- where the risk and/or risk profile associated with the Customer and the nature of the Business Relationship gives reason for the performance of additional actions in order to be able to appropriately monitor the Business Relationship later.

If the Customer is a legal entity, in addition to aforementioned the Company shall identify the Customer´s area of activity, where the Company shall understand what the Customer deals with and intends to deal with in the course of the Business Relationship and how this corresponds to the purpose and nature of the Business Relationship in general and whether it is reasonable, understandable and plausible.

The area of activity must fit into the experience profile of the Customer's representative (or key persons) and/or the Beneficial Owner. Thus, the Company has to identify where the representative's and/or Beneficial Owner's capacity, capability, skills and knowledge (experience in general) comes from in order to operate in this area of activity, with these business volumes and with these main business partners.

5.8. Monitoring of the business relationship

The Company shall monitor established Business Relationships where the following ongoing due diligence (ODD) measures are implemented:

- ensuring that the documents, data, or information collected in the course of the application of due diligence measures are updated regularly and in the case of trigger events, i.e., primarily the data concerning the Customer, their representative (incl. the right of representation) and Beneficial Owner as well as the purpose and nature of the Business Relationship;
- ongoing monitoring of the Business Relationship, which covers transactions carried out in the business relationship to ensure that the transactions correspond to the Company's knowledge of the Customer, their activities and risk profile;
- identification of the source and origin of funds used in the transaction(s).

The Company shall regularly check and update the documents, data and information

collected within the course of the implementation of CDD measures and update the Customer's risk profile.

The regularity of the checks and update must be based on the risk profile of the Customer and the checks must take place at least:

- once per month for the high-risk profile Customer;
- once semi-annually for the medium-risk profile Customer;
- once annually for the low-risk profile Customer.

The collected documents, data and information must also be checked if an event has occurred which indicates the need to update the collected documents, data and information.

In the course of the ongoing monitoring of the Business Relationship, the Company shall monitor the transactions concluded during the Business Relationship in such a manner that the latter can determine whether the transactions to be concluded correspond to the information previously known about the Customer (i.e., what the customer declared upon the establishment of the Business Relationship or what has become known in the course of the Business Relationship).

The Company shall also monitor the Business Relationship to ascertain the Customer's activities or facts that indicate criminal activities, Money Laundering or Terrorist Financing or the relation of which to Money Laundering or Terrorist Financing is probable, incl. complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or that are uncharacteristic of the specific features of the business in question.

In the course of the Business Relationship, the Company shall constantly assess the changes in the Customer's activities and assess whether these changes may increase the risk level associated with the Customer and the Business Relationship, giving rise to the need to apply EDD measures.

In the course of the ongoing monitoring of the Business Relationship, the Company applies the following measures:

- screening i.e., monitoring transactions in real-time;
- monitoring i.e., analyzing transactions later.

The objective of screening is to identify:

- suspicious and unusual transactions and transaction patterns;
- transactions exceeding the provided thresholds;
- politically exposed persons and circumstances regarding Sanctions.

The screening of the transactions is performed automatically and includes the following measures:

- established thresholds for the Customer's transactions, depending on the Customer's risk profile and the estimated transactions turnover declared by the Customer;
- the scoring of Crypto-assets wallets where the Crypto-assets shall be sent in accordance with the Customer's order;
- the scoring of Crypto-assets wallets from which the Crypto-assets is received.

If the Customer gives request for a transaction which exceeds the threshold established or for transaction to the Crypto-assets wallet with high-risk score (e.g. wallets related to fraud, crime, etc.), the transaction shall be manually approved by the Employee, who shall assess, before the approval, the necessity to apply any additional CDD measures (e. g. applying EDD measures, asking source and origin of funds or asking additional information regarding the transaction).

When monitoring transactions the Employee shall assess transaction with a view to detect activities and transactions that:

- deviate from what there is reason to expect based on the CDD measures performed, the services provided, the information provided by the Customer and other circumstances (e.g. exceeding estimated transactions turnover, Crypto-asset sending each time to new Crypto-asset wallet, volume of transactions exceeding limit);
- without deviating according to previous clause, may be assumed to be part of a Money Laundering or Terrorist Financing;
- may affect the Customer's risk profile score.

In the case, where the aforementioned fact is detected, the Employee shall notify MLRO and postpone any transaction of the Customer until MLRO's decision regarding this.

In addition to aforementioned, the MLRO shall review the Company's transactions regularly (at least once per day) to ensure that:

- the Company's Employees properly performed the aforementioned obligations;
- there are no transactions and transaction patterns that are complicated, high-value and unusual and that have no reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features.

The Company identifies the source (8) and origin (9) of the funds used in transaction(s) if necessary. The need to identify the source and origin of funds depends on the Customer's previous activities as well as other known information.

Thereby the identification of the source and origin of the funds used in transaction shall be performed in the following cases:

- the transactions exceed the limits established by the Company;
- the transactions do not correspond to the information previously known about the Customer;

- the Company wants to or should reasonably consider it necessary to assess whether the transactions correspond to the information previously known about the Customer;
- the Company suspects that the transactions indicate criminal activities, Money Laundering or Terrorist Financing or that the relation of transactions to Money Laundering or Terrorist Financing is probable, incl. complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

The company actively monitors and detects linked transactions that may be structured to avoid detection under the EUR 1,000 threshold.

Transfers conducted within a short timeframe and involving the same or related parties are flagged for review.

Transactions structured across multiple accounts or involving seemingly unrelated counterparties are assessed for possible threshold evasion.

A structured escalation and reporting process is in place for suspicious activities, ensuring compliance with regulatory requirements.

6. IMPLEMENTATION OF SANCTIONS

Upon the entry into force, amendment or termination of Sanctions, the Company shall verify whether the Customer, their Beneficial Owner or a person who is planning to have the Business Relationship or transaction with them is a subject of Sanctions.

If the Company identifies a person who is a subject of Sanctions or that the transaction intended or carried out by them is in breach of Sanctions, the Company shall apply Sanctions and inform the GIIF thereof immediately but no later than within 2 work days

6.1. Procedure for identifying the subject of Sanctions and a transaction violating Sanctions

The Company shall use at least, but not limited to the following sources (databases) to verify the Customer's relation to Sanctions:

- https://www.sanctionsmap.eu/
- https://scsanctions.un.org/search/

In addition to aforementioned sources, the Company may use any other sources by the decision of the Employee who is applying CDD measures.

To verify that the persons' names resulting from the inquiry are the same as the persons listed in a notification containing Sanction(s), their personal data shall be used, the

main characteristics of which are, for a legal entity, its name under which the legal entity is registered, legal entity identifier (LEI) or a registration number, if such number has been issued, and for a natural person, their full name and surname as they appear in the customer's identity document and official personal number or date of birth..

In order to establish the identity of the persons specified in the relevant legal act or notice being the same as those identified as a result of the inquiry from databases, the Company must analyze the names of the persons found as a result of the inquiry based on the possible effect of factors distorting personal data (e. g. transcribing foreign names, different order of words, substitution of diacritics or double letters etc.).

The Company shall perform above mentioned verification on an ongoing basis in the course of an established Business Relationship.

The frequency of the ongoing verifications depends on the Customer's risk profile:

- once per day for the high-risk profile Customer;
- once per week for the medium-risk profile Customer;
- once per month for the low-risk profile Customer.

If the Employee has doubts that a person is a subject of Sanctions, the Employee shall immediately notify the MLRO or the Management Board member. In this case the MLRO or the Management Board member shall decide whether to ask or acquire additional data from the person or notify the relevant authority immediately of their suspicion.

The Company shall primarily acquire additional information on their own about the person who is in Business Relationship or is performing a transaction with them, as well as the person intending to establish the Business Relationship, perform a transaction or an act with them, preferring information from a credible and independent source.

If, for some reason, such information is not available, the Company shall ask the person who is in the Business Relationship or is performing a transaction or an act with them, as well as the person intending to establish a Business Relationship, perform a transaction or an act with them, whether the information is from a credible and independent source and assess the answer.

6.2. Actions when identifying the Sanctions subject or a transaction violating Sanctions

If the Employee of the Company becomes aware that the Customer which is in Business Relationship or is performing a transaction with the Company, as well as a person intending to establish the Business Relationship or to perform a transaction with the Company, is the subject of Sanctions, the Employee shall immediately notify the MLRO or the Management Board member, about the identification of the subject of Sanctions, of the doubt thereof and of the measures taken.

The MLRO or the Management Board member shall refuse to conclude a transaction or proceeding, shall take measures provided for in the act on the imposition or implementation of the Sanctions and shall notify immediately the GIIF of their doubts and of the measures taken.

When identifying the subject of the Sanctions, it is necessary to identify the measures that are taken to Sanction this person. These measures are described in the legal act implementing the Sanctions, therefore it is necessary to identify the exact sanction that is implemented against the person to ensure legal and proper application of measures.

7. REFUSAL TO THE TRANSACTION OR BUSINESS RELATIONSHIP AND THEIR TERMINATION

The Company is prohibited to establish a Business Relationship and the established Business Relationship or transaction shall be terminated (unless it is objectively impossible to do) in case when:

- the Company suspects Money Laundering or Terrorist Financing;
- it is impossible for the Company to apply the CDD measures, because the Customer does not submit the relevant data or refuses to submit them or the submitted data gives no grounds for reassurance that the collected data are adequate;
- the Customer whose capital consists of bearer shares or other bearer securities wants to establish the Business Relationship;
- the Customer who is a natural person behind whom is another, actually benefiting person, wants to establish the Business Relationship (suspicion that a person acting as a front is used);
- the Customer's risk profile has become inappropriate with the Company's risk appetite (i. e. the Customer's risk profile level is “prohibited”).
- If the information for crypto-asset transfers is incomplete or missing.

The Company treats information as missing if fields are left empty, or if the information provided is meaningless or incomplete.

The Company treats at least the following information as meaningless:

- strings of random or illogical characters (such as ‘xxxxx’, or ‘ABCDEFG’);
- use of titles (such as Dr or Mrs) without the person’s name;
- other designations that are incoherent or unintelligible (such as ‘An Other’, or ‘My Customer’).

Where the Company decides to reject a transfer or to return a transfer instead of requesting the missing information, the Company informs the prior relevant institution or service provider in the transfer chain that the transfer has been rejected or returned because of missing information

Where the rejection is technically not possible, the transfer is returned to the originator. Where returning the transfer to the original address is not possible, the Company

holds the returned assets in a secure, segregated account while communicating with the originator to arrange a suitable return method to the originator.

Where the Company requests required information that is missing, a reasonable deadline is set by which the information should be provided. As a general rule, this deadline shall not exceed three (3) working days for transfers within comparable regulatory environments and five (5) working days for cross-border transfers,, starting from the day the Company identifies the missing information. Longer deadlines up to seven days may be set where transfer chains involve:

- more than two parties in the transfer flow, including intermediaries and non-banks;
- counterparties established in jurisdictions outside those applying comparable AML/CTF standards. .

Where the Company decides to request the required information from the prior institution or service provider involved in the transfer chain it notifies such party in the transfer chain of the technical actions taken on that transfer due to missing or incomplete information, as applicable.

Any request for information or clarification is sent through the same messaging system that is used for transmitting the required information or, where technical limitations exist secure methods of contact are used in line with applicable data protection requirements..

Where the requested information is not provided within the specified deadline, the Company may issue a reminder and inform the relevant counterparty of the potential consequences of continued non-compliance.

Where the requested information is not provided by the set deadline, the Company makes the decision on whether to reject, return, suspend or execute the transfer in line with its risk-based policies and procedures. In addition to that decision it will, irrespective of whether the failure was repeated or not, consider the future treatment of the prior institution or provider in the transfer chain for AML/CFT compliance purposes, including rejecting any future transfers from or to the prior institution or provider or self-hosted address in the transfer chain, or restricting or terminating its business relationship with it.

Requests for missing information or clarification with respect to transfers from or to self-hosted addresses are sent directly to the Company's customer.

Repeated failures to provide required information result in the termination of the business relationship with the non-compliant counterparty.

Before taking the decision to terminate a business relationship,the Company will consider whether or not the risk can be managed in other ways, including ex ante through the application of enhanced due diligence measures.

In case of repeated failures to provide required information the Company will report

to the competent authority without undue delay, and no later than three months after identifying the repeatedly failing institution or provider. Reporting will take place regardless of the reasons given by the 'repeatedly failing' institution or provider if any, to justify that breach, or their location in the Union or outside.

In the event of a termination of the Business Relationship in accordance with this chapter, the Company shall transfer the Customer's assets within reasonable time, but preferably not later than within one month after the termination and as a whole to an account opened regulated financial institution.In exceptional cases, assets may be transferred to an account other than the Customer's account or issued in cash. Irrespective of the recipient of the funds, the minimum information given in English in the payment details of the transfer of the Customer's assets is that the transfer is related to the extraordinary termination of the Customer relationship.

The Company will not accept as Customers, persons or entitled from Afghanistan, Barbados, Belarus, Bolivarian Republic of Venezuela, Burkina Faso, Burma (Myanmar), Cambodia, Cameroon, Cayman Islands, Central African Republic, Crimea (region of Ukraine), Cuba, Democratic Republic of the Congo, Democratic People's Republic of Korea, Donetsk (region of Ukraine), Egypt, Ethiopia, Gibraltar, Haití, Iran, Iraq, Jamaica, Jordan, Kherson (region of Ukraine), Libya, Lebanon, Luhansk (region of Ukraine), Mali, Morocco, Mozambique, Nepal, Nigeria, Nicaragua, Pakistan, Panama, Philippines, People's Republic of China, Russia, Senegal, Somalia, South Africa, South Sudan, Sudan, Syria, Tanzania, Trinidad and Tobago, Uganda, United Arab Emirates, Vanuatu, Vietnam, Yemen, Zaporizhzhia (region of Ukraine), Zimbabwe.

8. REPORTING OBLIGATION

The Company must suspend the transaction disregarding the amount of the transaction (except for the cases where this is objectively impossible due to the nature of the Monetary Operation or transaction, the manner of execution thereof or other circumstances) and through its MLRO must report to the GIIF on the activity or the circumstances that they identify in the course of economic activities and whereby:

- the Company has established that the Customer is carrying out a suspicious transaction;
- the Company knows or suspects that assets of any value are obtained directly or indirectly from criminal activity or participation in such activity.

The reports specified above must be made before the completion of the transaction if the Company suspects or knows that Money Laundering or Terrorist Financing or related crimes are being committed and if said circumstances are identified before the completion of the transaction.

If the necessity of the above mentioned report arises, the Employee to whom such necessity became known must immediately notify the MLRO about this.

In any case (i.e. also in the situation where an activity or circumstance is identified after the completion of the transaction), the reporting obligation for the above reports must be performed immediately, but not later than three working hours after the identification of the activity or circumstance or the emergence of the actual suspicion (i.e. the situation where the suspicion cannot be dispelled).

8.1. Reporting obligation regarding specific types of transactions

The Company through its MLRO must send information to the supervisory authority not later than within 7 working days after the identification of a crypto-asset transaction performed if the amount of the client's single transaction with crypto-assets or several interconnected transactions with crypto-assets is equal to or exceeds 15,000 euros or the equivalent amount in foreign currency.

In case specified above information submitted to the supervisory authority shall include, as applicable:

- the data confirming the Customer's identity, and where the transaction is carried out through a representative – also the data confirming the identity of the representative;
- the amount of the transaction;
- the currency in which the transaction was executed;
- the date of execution of the transaction;
- the manner of execution of the Monetary Operation;
- the entity for whose benefit the Monetary Operation was executed (if it's possible);
- other data specified in the relevant supervisory authority's instructions.

All the reports described in this chapter shall be sent in accordance with the Company's reporting guidelines through a secure channel ensuring full confidentiality (one of the annexes of these Guidelines).

The Company, a structural unit of the Company, a Management Board member, MLRO and the Employee is prohibited to inform a person, its Beneficial Owner, representative or third party about a report submitted on them to the supervisory authority, a plan to submit such a report or the occurrence of reporting as well as about a precept made by the supervisory authority or about the commencement of criminal proceedings.

9. TRAINING OBLIGATION

The Group ensures that its Employees, its contractors and others participating in the business on a similar basis and who perform work tasks that are of importance for preventing the use of the Company's business for Money Laundering or Terrorist Financing ('Relevant Persons') have the relevant qualifications for these work tasks.

When a Relevant Person is recruited or engaged, the Relevant Person's

qualifications are checked as part of the recruitment/appointment process by carrying out background checks, which is documented using a special standard form assessing Employee suitability.

In accordance with the requirements applicable to the Group on ensuring the suitability of Relevant Persons, the Group makes sure that such persons receive appropriate training and information on an ongoing basis to be able to fulfill the Group's obligations in compliance with the applicable legislation. It is ensured through training that such persons are knowledgeable within the area of AML/CFT to an appropriate extent considering the person's tasks and function. The training must provide, first and foremost, information on all the most contemporary money laundering and terrorist financing methods and risks arising therefrom.

This training refers to relevant parts of the content of the applicable rules and regulations, the Group's risk assessment, the Group's Guidelines and procedures and information that should facilitate such Relevant Persons detecting suspected Money Laundering and Terrorist Financing. The training is structured on the basis of the risks identified through the risk assessment policy.

The content and frequency of the training is adapted to the person's tasks and function on issues relating to AML/CFT measures. If the Guidelines is updated or amended in some way, the content and frequency of the training is adjusted appropriately.

For new Employees, the training comprises a review of the content of the applicable rules and regulations, the Group's risk assessment policy, these Guidelines and other relevant procedures.

The Employees and the Management Board members receive training on an ongoing basis under the auspices of the MLRO in accordance with the following training plan:

- periodicity: at least once a year for the Management Board members. At least once a year for the Group's Employees and Relevant persons engaged.
- scope: review of applicable rules and regulations, the Group's Guidelines and other relevant procedures. Specific information relating to new/updated features in the applicable rules and regulations. Report and exchange of experience relating to transactions reviewed since the previous training.

In addition to the above, Relevant Persons are kept informed on an ongoing basis about new trends, patterns and methods and are provided with other information relevant to the prevention of Money Laundering and Terrorist Financing. The training held is to be documented electronically and confirmed with the Relevant Person signature. This documentation should include the content of the training, names of participants and date of the training.

10. COLLECTION AND STORING OF DATA, LOGBOOKS

The Company automatically or through the person (incl. Employees, Management

Board members and MLRO) who firstly receives the relevant information or documents shall register and retain the following data:

- all data collected within CDD measures implementation;
- information about the circumstances of refusal of the establishment of the Business Relationship by the Company;
- the circumstances of the refusal to establish Business Relationship on the initiative of the Customer if the refusal is related to the application of CDD measures by the Company;
- information on all of the operations made to identify the person participating in the transaction or the Customer´s Beneficial Owner;
- information if it is impossible to perform the CDD measures;
- information on the circumstances of termination of the Business Relationship in connection with the impossibility of application of the CDD measures
- each transaction date or period and a description of the contents of the transaction, in accordance with the Company's Policy on record-keeping of crypto-asset services, activities, orders and transactions.
- information serving as the basis for the reporting obligations specified in the Guidelines;
- data of suspicious or unusual transactions or circumstances of which the supervisory authority was not notified (e. g. complex or unusually large transactions, transactions conducted in an unusual pattern and transactions that do not have an apparent economic or lawful purpose, Business Relationships or Monetary Operations with customers from Third Countries where measures to prevent Money Laundering and/or Terrorist Financing are insufficient or do not meet international standards according to information officially published by international intergovernmental organizations);
- information about Originator and Beneficiary of crypto-asset transactions.

Some of the data specified above shall be entered in the logbook (as described below) in chronological order on the basis of documents confirming a Monetary Operation or transaction or other legally valid documents related to the execution of Monetary Operations or transactions, immediately, but not later than within 3 business days after the execution of a Monetary Operation or transaction.

The data specified above shall be retained for the time frame as set out in the applicable regulatory requirements, but not less than for a 5 year period after the expiry of the Business Relationship or the completion transaction.

The correspondence of a Business Relationship with the Customer must be retained for the time frame as set out in the applicable regulatory requirements, but not less than for a 5 year period from the date of termination of transactions or Business Relationship.

Documents and data must be retained in a manner that allows for exhaustive and immediate response to the queries made by supervisory authorities, investigation

authorities or the court.

The Company implements all rules of protection of personal data upon application of the requirements arising from the applicable law.The Company is allowed to process personal data gathered upon CDD implementation only for the purpose of preventing Money Laundering and Terrorist Financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

The Company deletes the retained data after the expiry of the time period, unless the legislation regulating the relevant field establishes a different procedure. On the basis of a precept of the competent supervisory authority, data of importance for prevention, detection or investigation of Money Laundering or Terrorist Financing may be retained for a longer period, but not for more than two years after the expiry of the first time period.

The company retains all relevant transaction records, including payer/originator and payee/beneficiary details, in compliance with applicable AML/CTF and data protection requirements.

All AML-relevant transaction data is stored for the time frame as set out in the regulatory requirements applicable to the Company, but not less than for a 5 year period from the date of the transaction.

Records are maintained in a secure, tamper-proof system to ensure their integrity and accessibility for regulatory audits.

10.1. Registration logbooks keeping

For the purposes of performing AML obligations, the Company shall keep (complete) the following registration logbooks reflecting Monetary Operations and transactions (hereinafter – logbooks):

- logbook of single or several interrelated monetary transactions the amount of which is equal to or exceeds 15,000 euros or its equivalent in foreign currency, regardless of whether the transaction is carried out in the form of one or several related transactions and suspicious monetary transactions and their reports;
- logbook of the Customers with whom transactions or Business Relationships were refused or terminated under the circumstances related to violations of the procedure for the prevention of Money Laundering and/or Terrorist Financing.

Registration logbook of reports, suspicious Monetary Operations and transactions shall include the following in chronological order:

- data confirming the identity of the Customer and their representative (if the monetary transaction is performed or the transaction is concluded through a representative): name and surname of a natural person, personal identification code or date of birth , citizenship;
- if applicable, which criteria in accordance with the regulatory requirements for the

Company, according to which it is recognized that a monetary operation or transaction is considered suspicious, does the operation or transaction meet;

- method of completion of suspicious Monetary Operation or transaction;
- date and time of suspicious monetary operation or transaction, characterization of assets subject to transaction (cash etc.), and its value (amount of money, currency used for conduct of Monetary Operation or transaction, asset market value);
- the data on the transaction beneficiary(ies): full name and surname as they appear in the customer's identity document and official personal number or, alternatively, the date of birth , and in case of legal entity, name under which the legal entity is registered, legal form legal entity identifier (LEI) or a registration number, if such number has been issued;
- contact details of the Customer: phone number(s), e-mail address(es), contact person(s), their phone numbers, email addresses,
- description of assets that the Customer cannot control or use from the moment of suspension of suspicious monetary transaction or transaction (place and other information characterizing assets);
- in the event of a suspicious monetary transaction or transaction has not been suspended, relevant reasons;
- methods of account management;
- other relevant details, according to the Employee's decision.

The Company shall include in the registration logbook of customers, where transactions or Business Relations have been terminated the following, in chronological order:

- data confirming the identity of the Customer and their representative (if the monetary transaction is performed or the transaction is concluded through a representative): name and surname of a natural person, personal identification code or date of birth , citizenship;
- data on the monetary transaction or transaction: the date of the transaction, description of the assets subject to the transaction (cash, real estate, Virtual Currency etc.) and its value (amount of money, currency in which the monetary transaction or transaction is performed, market value of the assets, etc.);
- in the case of crypto-asset transactions or transactions, it is not objectively possible to identify the payee, other information enabling the crypto-asset address to be linked to the identity of the crypto-asset owner: Internet Protocol (IP) address, e-mail address, etc.;
- in the case of crypto-asset transactions crypto-asset Address(es) related to transaction and transaction hash(es);
- the data on the Customer's beneficiary(ies): full name and personal ID number of a natural person (in case of a foreigner: full name and surname as they appear in the customer's identity document and official personal number or, alternatively, the date of birth), and in case of legal entity, name under which the legal entity is registered, legal form legal entity identifier (LEI) or a registration number, if such number has

been issued;
- reasons for termination of transactions or Business Relations pertaining to breaches of procedure of prevention of Money Laundering and/or Terrorist Financing.

11. INTERNAL CONTROL OF EXECUTION OF THE GUIDELINES

The performance of the Guidelines shall be internally controlled by the Company's head of the management board responsible for Company's adherence to applicable regulatory requirements in the field of AML/CTF(hereinafter in this chapter – Head of the Management Board).

The Head of the Management Board must have the required competency, tools, and access to the relevant information in all structural units of the Company.

The Head of the Management Board shall perform internal control functions at least in the following fields:

- the Company's compliance with established risk assessment policy and risk appetite;
- CDD measures implementation;
- implementation of Sanctions;
- the Company's obligation to refusal to the transaction or business relationship and their termination;
- the Company's reporting obligation to the supervisory authority;
- the Company's training obligation regarding the AML/CFT requirements;
- the Company's obligation for collection and preservation of data.

The exact measures for performing internal control shall be determined by the Head of the Management Board and must correspond to the Company's size and its nature, scope and level of complexity of the activities and services provided.

The Head of the Management Board must consider at least examination fields specified above. The internal control measures shall be performed at the time determined by the Head of the Management Board with the frequency set by him or her, at least once per month, if the nature of measure does not expressly provide otherwise.

The results of internal control measures implementation (hereinafter in this chapter – the Internal Control Data) shall be saved separately from other data and retained for 5 years.

Only Management Board members may have access to the Internal Control Data. Head of the Management Board may provide access to the Internal Control Data to other Employees or third parties (e. g. advisors, auditors, etc.) only with prior consent of the Management Board. The persons who have access to the Internal Control Data must not disclose it to anyone without prior consent of the Management Board.

The Internal Control Data shall be saved in chronological order with format, which allows to analyze this and understandably connect this to other relevant data.

The Head of the Management Board shall provide the internal control report to the Management Board at least quarterly and to the general meeting of the Company's shareholders at least annually.

The provided internal control report shall include at least the following:

- period of exercising the internal control;
- name and position of the person executing the internal control;
- description of the internal control measures that has been performed;
- results of the internal control;
- general conclusions from the exercised internal control;
- determined deficiencies, which were eliminated in the period of exercising the internal control;
- determined deficiencies, which were not eliminated at the end of period of exercising the internal control;
- measures that are required to implement for elimination of determined deficiencies.

The Management Board shall review the internal control report provided and make a resolution regarding it. The Head of the Management Board shall be notified about the essence of such resolution in format which can be reproduced in writing. For this reason, the Management Board is obliged to:

- analyze the results of performed internal control;
- implement actions to eliminate deficiencies occurred.

The Company must review and, if necessary, update internal control procedure at least annually and in the following cases:

- following the publication of supranational or international money laundering and terrorist financing risk assessments issued by relevant authorities or organizations;
- following the publication of national money laundering and terrorist financing risk assessments in jurisdictions where the Company operates;
- upon receipt of instructions or guidance from competent supervisory or regulatory authorities to strengthen applicable internal control procedures;
- in the event of significant events or changes in the management, business activities, or operations of the Company, Group or the Services.

Explanatory Notes

1. where an identity document does not contain data on the customer's citizenship, financial institutions and other obliged entities must, when identifying the customer that is a natural person in the physical presence of the customer, require the customer to provide the data on citizenship.

2. where an identity document does not contain data on the customer's citizenship, financial institutions and other obliged entities must, when identifying the customer that is

a natural person in the physical presence of the customer, require the customer to provide the data on citizenship.

3. direct ownership is a manner of exercising control whereby the natural person owns a 25 percent shareholding plus one share or an ownership right of over 25 percent in the company.

4. indirect ownership is a manner of exercising control whereby a 25 percent shareholding plus one share or an ownership right of over 25 percent in the company is owned by a company that is controlled by a natural person or several companies that are controlled by the same natural person.

5. a member of senior management is a person who makes the strategic decisions that fundamentally affect business activities and/or practices and/or the company general (business) trends or in its absence carries out everyday or regular management functions of the company within the scope of executive power (e.g. chief executive officer (CEO), chief financial officer (CFO), director or president, etc.).

6. family member means the spouse, the person with whom partnership has been registered (i.e. the cohabitant), parents, brothers, sisters, children and children's spouses, children's cohabitants.

7. close associate means a natural person who, together with PEP, is a member of the same legal entity or of a body without legal personality or maintains other business relationship; or a natural person who is the only the Beneficial Owner of the legal entity or a body without legal personality set up or operating de facto with the aim of acquiring property or another personal benefit for the PEP.

8. the source of the funds used in the transaction is reason, explanation and basis (legal relationship and its content) why the funds were transferred.

9. the origin of the funds used in the transaction is the activity by which the funds were earned or received as described in the relevant chapter of these Guidelines.

Dated: May 5th, 2026