UAB CHRONOS GLOBAL
Eišiškių Sodų 18-oji g. 11
Vilnius, Lithuania
info@columis.com

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING COMPLIANCE GUIDELINES

(the AML/CTF Policy)

INTRODUCTION

The purpose of these Guidelines for Anti-Money Laundering (AML), Combating Terrorist Financing (CTF), and Sanctions measures is to ensure that **UAB Chronos Global** (the **Company**) has internal guidelines to prevent the use of its business for Money Laundering and Terrorist Financing and internal guidelines for implementation of international sanctions. Whereas. These Guidelines are of a general nature, they are equaled to the AML/CTF Policy of the Company.

These Guidelines have been adopted to ensure that the Company complies with the rules and regulations set out in the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania (the **Law**) and other applicable legislation, including but not limited to the following:

- Guidelines of the European Banking Authority regarding remote customer identification solutions in accordance with Article 13(1) of Directive (EU) 2015/849 (hereinafter – **EBA Remote Onboarding Guidelines**)[1].
- Technical Requirements for the Customer Identification Process for Remote Identification Authentication via Electronic Devices for Direct Video Transmission approved by the Director of the Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania on the 30th of November 2016 by Resolution No. V-314 "For the Technical Requirements for the Customer Identification Process for Remote Identification Authentication via Electronic Devices for Direct Video Transmission" (hereinafter – the **Technical Requirements**).[2]
- Resolution No. V-240 of the 5th of December 2014 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania "On the Approval of the List of Criteria for Money Laundering and Suspicious or Unusual Monetary Operations or Transactions Identification"[3].
- Resolution No. V-5 of the 10th of January 2020 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania "On the Approval of Guidelines for the Depositary virtual currency wallet operators and virtual currency exchange operators to prevent money laundering and/ or terrorist financing"[4].
- Resolution No. V-273 of the 20th of October of 2016 of the Director of Financial Crime Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania "On the Approval of

[1] https://www.eba.europa.eu/legacy/regulation-and-policy/regulatory-activities/anti-money-laundering-and-countering-financing-4#activity-versions
[2] https://www.e-tar.lt/portal/lt/legalAct/e45f4270b70011e6aae49c0b9525cbbb/asr
[3] https://www.e-tar.lt/portal/lt/legalAct/a664b2107ecd11e4bc68a1493830b8b9
[4] https://www.e-tar.lt/portal/lt/legalAct/570a231035e011ea829bc2bea81c1194

Guidelines for the Supervision of Financial Crimes for the Implementation of International Financial Sanctions in the Field of Regulations of the Ministry of Internal Affairs of the Republic of Lithuania"[5].

- Order No. 1V-701 of the Minister of the Interior of the Republic of Lithuania of the 16th of October 2017 "On Suspension of Suspicious Monetary Transactions or Transactions and Submission of Information on Suspicious Monetary Transactions or Transactions to the Financial Crime Investigation Service under the Description of Procedure of the Ministry of the Interior of the Republic of Lithuania and Information on Cash Transactions or Transactions equal to or exceeding 15,000 euros or submission of the corresponding amount in foreign currency to the Financial Crime Investigation Service under the approval of the description of the procedure of the Ministry of the Interior of the Republic of Lithuania"[6].
- Order No. V-129 of the Director of the Financial Crime Investigation Service of the 21st of May 2015 by "On Approval of Information Forms, Submission Schemes and Recommendations for Completion of Information Provided in Accordance with the Requirements of the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania"[7].
- Order No. V-131 of the Director of the Financial Crime Investigation Services under the Ministry of the Interior of the Republic of Lithuania regarding the Approval of the Description of the Procedure for Approval and Submission of a Copy of an Identity Document.[8]
- Order No V-314 of the Director of the Financial Crime Investigation Services under the Ministry of the Interior of the Republic of Lithuania on Technical Requirements for the Customer Identification Process for Remote Identification using Electronic Means of Direct Image Transmission[9].
- Resolution of the Board of the Bank of Lithuania regarding Approval of Instructions to Financial Market Participants to Prevent Money Laundering and/or Terrorist Financing No 03-15[10].
- Order of the Minister of the Interior of the Republic of Lithuania regarding the Suspension of Suspicious Monetary Transactions or Transactions and Submission of Information on Suspicious Monetary Transactions or Transactions to the Financial Crime Investigation Service under the Description of the Procedure of the Ministry of the Interior of the Republic of Lithuania and Submission of Information on Cash Transactions or Transactions in the Amount Equivalent to or Exceeding EUR 15,000 or the Equivalent Amount in Foreign Currency to the Financial Crime Investigation Service under the Approval of the Description of the Procedure of the Ministry of the Interior of the Republic of Lithuania No 1V-701[11].
- Director Order of the Financial Crime Investigation Services under the Ministry of the Interior of the Republic of Lithuania on regarding the Approval of the Instructions for the Proper Implementation of

[5] https://www.e-tar.lt/portal/lt/legalAct/01d5d4e0974411e69ad4c8713b612d0f
[6] https://e-tar.lt/portal/lt/legalAct/143ad320b24011e7afdadfc0e4460de4
[7] https://www.e-tar.lt/portal/lt/legalAct/e1f42fa0006d11e588da8908dfa91cac/asr
[8] https://www.e-tar.lt/portal/lt/legalAct/42a3a4e099e911e78871f4322bb82f27
[9] https://www.e-tar.lt/portal/lt/legalAct/e45f4270b70011e6aae49c0b9525cbbb/asr
[10] https://www.e-tar.lt/portal/lt/legalAct/7e124670b68511e4bcec9ef1757ec710/asr
[11] https://www.e-tar.lt/portal/lt/legalAct/143ad320b24011e7afdadfc0e4460de4/asr

International Financial Sanctions under the Supervision of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania No V-273[12].

These Guidelines are subject to a review by the AML Compliance Officer (or person conducting relevant functions) and the Management Body of the Company at least annually. Proposal for a review and the review of these Guidelines may be scheduled more frequently by the decision of the Company's Money Laundering Reporting Officer (MLRO) or the Internal Control Officer.

These Guidelines shall be accepted and approved by the resolution of the Company's Management Body.

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 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 person, exceeds 25 percent, including holdings in the form of shares or other forms of bearer.

Business Relationship means a relationship that is established upon conclusion of a long-term contract by the Company in economic or professional activities for the purpose of provision of a service or distribution thereof in another manner or that is not based on a long-term contract, but whereby a certain duration could be reasonably expected at the time of establishment of the contact and during which the Company repeatedly makes separate transactions in the course of economic or professional activities while providing a service.

Company means legal entity with following data:

- company name: UAB Chronos Global;
- registration country: Lithuania;
- registration number: 305947127;
- address: Eišiškių Sodų 18-oji g. 11, Vilnius;
- email: info@columis.com

Custodian Virtual Currency Wallet means Virtual Currency Address(es) generated with the public key[13] for storing and managing Virtual Currencies entrusted to the Company but remaining their property.

Customer means a natural person or a legal entity which has the Business Relationship with the Company or a natural person or legal entity with which the Company enters into the Occasional Transaction.

[12] https://www.e-tar.lt/portal/lt/legalAct/01d5d4e0974411e69ad4c8713b612d0f/asr
[13] **Public key** means a code of letters, numbers and/or symbols designed to identify the customer and generate the client's Virtual Currency Address

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

Guidelines – this document including all annexes as provided above. The Guidelines include inter alia the Company's internal control procedure regarding the Guidelines and the Company's risk assessment policy regarding risk-based approach for ML/TF risks.

Management Board means the management board of the Company. If the Company has no management board – the Manager (Head) of the Company shall be considered as the Management Board member and he or she shall be responsible for the Management Board duties in the context of the Guidelines.

MLRO means Money Laundering Reporting Officer, who is appointed to the Company as a person responsible for receiving internal disclosures and making reports to the Financial Crime Investigation Service (FCIS) and other duties as described above.

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 main 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.

Occasional Transaction means the transaction performed by the Company in the course of economic or professional activities for the purpose of provision of a service or sale of goods or distribution thereof in another manner to the Customer outside the course of an established Business Relationship.

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. Sanctions shall consist of the following:

- 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 imposing obligations on Lithuania;

- Sanctions of the Government of the Republic of Lithuania, which is a tool of foreign policy which may be imposed in addition to the objectives specified in previous clause in order to protect the security or interests of Lithuania.

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.

Third Country – means a state that is not a member state of the European Economic Area (EEA).

Virtual Currency means a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4(25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, pp 35–127) or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same Directive.

Virtual Currency Address means address/account generated from letters, numbers and/or symbols in the blockchain, by which the blockchain allocates the Virtual Currency to the owner or recipient.

PRINCIPLES FOR STRUCTURE AND MANAGEMENT OF THE COMPANY

The organizational structure of the Company 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 Company must correspond to the complete understanding of potential risks and their management. The reporting and subordination chains of the Company must be ensured in such a way that all Employees know their place in the organizational structure and know their work duties.

The Management Board

The Management Board in the Company is not formed. Therefore, one of the Management Bodies, i.e. the Head of the Company, assumes the obligations of the Management Board in the context of the Guidelines, and acts as the carrier of the culture of compliance with the requirements of Money Laundering and Terrorist Financing prevention, guarantees that the Employees and partners 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 Head of the Company bears the ultimate responsibility for the measures taken to prevent the use of the Company's services for Money Laundering or Terrorist Financing. He provides oversight and is responsible for:

- establishing and maintaining AML[14] processes, procedures, risk, and control processes;
- adopting these Guidelines and other internal guidelines and instructions;
- approving the Company's Guidelines for AML measures;
- appointing the 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.

The first line of defense – the Employees

The first line of defense has the function of applying due diligence measures upon Business Relationship and Occasional Transactions and applying due diligence measures during the Business Relationship. First line of defense comprises the structural units and Employees of the Company with whose activities risks are associated and that must identify and assess these risks, their specific features and scope and that

[14] For the purpose of simplifying these Guidelines, relation to "AML" includes also prevention of terrorism financing and implementation of Sanctions

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 Company belong to the first line of defense. They are the managers (owners) of these risks and responsible for them.

The Employees of the Company 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 Company, and ensure that the country'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 functions and accountability;
- 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.

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 Company 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 Company.

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

Risk policy is implemented, and the risk management framework is controlled by the **risk management function**. The performer of the risk management function ensures that all risks are identified, assessed, measured, monitored, and managed, and informs the appropriate units of the Company about them. The performer of the risk management function for the purposes of AML primarily performs the supervision over adherence to risk appetite, supervision over risk tolerance, supervision over identification of changes in risks, performs the overview of associated risks, and performs other duties related to risk management.

The Management Board has appointed a **MLRO** for performing the second line of defense functions. This person is not operationally involved in the areas that the MLRO will be monitoring and verifying and is thus independent in relation to these. The MLRO is accountable for the following activities:

- prepare 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 Company's procedures and guidelines to prevent the use of the business for Money Laundering or Terrorist Financing are fit for purpose and effective.

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 Financial Crime Investigation Service (FCIS);
- number and content of a request for information from the FCIS within the framework of an investigation;
- confirmation that the Company'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.

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 Company's structural unit with the relevant functions or by the third party, which provides the relevant service to the Company.

The Employees, the Company's structural unit or a 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 Company. The internal audit methods must comply with the size of the Company, the nature, scope, and level of complexity of the activities and provided services, incl. the risk appetite and risks arising from activities of the Company.

The decision to conduct an internal audit is made by a resolution of the Management Board (Director's Resolution). The Management Body must assess the need to conduct an internal audit at least annually.

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.

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/updating of the Business Relationship and during the ongoing monitoring of the Business Relationship;
- upon executing or mediating Occasional Transaction(s) outside the Business Relationship, where the value of the transaction(s) amounts to 700 euros or more (or an equal amount in another asset) within 24 hours; however, the overall Customer's account activity is monitored in retrospective monitoring, and in case any suspicious activity is detected, then transaction minimum threshold of such Customer is removed;
- upon verification of information gathered while applying due diligence measures or in 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;
- before starting a business relationship or before carrying out a one-time monetary operation or transaction, when it is necessary to take measures and determine and verify the identity of the

Customer and the beneficiary, following Articles 13 and 14 of Regulation (EU) 2016/679, the Company shall provide the new/potential Customers with information about the processing of their data.

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 the required CDD measures;
- the Company has any suspicions that the Company's services or transactions will be used for Money Laundering or Terrorist Financing;
- the risk level of the Customer or of the transaction does not comply with the Company's risk appetite.

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

The Services Provided

The Company's main economic activity is the Virtual Currency services. For this reason, the Company offers to their Customers the following transaction types:

- providing Custodian Virtual Currency Wallet operator service, which allows to the Customer open Custodian Virtual Currency Wallet on the Customer's name and make transactions with this wallet: to deposit Virtual Currency and to withdraw deposited Virtual Currency to another wallet(s);
- providing Virtual Currency exchange operator service, which allows the Customer to exchange, purchase and sell Virtual Currency.

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 or its reliability and independence cannot be verified);
- 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;
- 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).

Identifying the Customer and verifying the Customer's identity on the basis of documents, data, or information obtained from a reliable and independent source, including, where available, electronic identification means, relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council or any other secure, remote or electronic identification process regulated, recognized, approved or accepted by the relevant national authorities.

For Customers and/or any of its Key Person is registered in high-risk FATF and/or EU countries, the Company cannot rely on data, documents, and any other information issued in those countries (general principal requirement). Therefore, in addition to documents and data from high-risk countries there is mandatory to rely on data and information from:

a) data and documents obtained from countries, other than the high-risk country(ies).

b) Results of the checking(s) in independent and reliable sources of information, meaning checking of the Customer's data and documents obtained not from high-risk countries.

Proof of the checking in independent and reliable sources of information is mandatory to collect and store for at least 8 years.

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[15] the following data of the Customer who is a natural person:

- name(s) and surname(s);
- personal identification number;[16] or

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

- business name or name;
- legal form;
- registration number, if such number has been issued;
- head office (address) and address of actual operation;
- 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.

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;

[15] When the Customer is state or municipal institution or agency, or the Bank of Lithuania, the Company may in the course of applying SDD measures collect only personal number of such entity´s and their representative.

[16] in case of a foreigner – date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification), the number and period of validity of the residence permit in the Republic of Lithuania and the place and date of its issuance (applicable to foreigners).

- 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, checking if the information provided is actual and up-to date.

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.

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 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 a Third Country;
- in case of preventing any Business Relationship with the PEP, the family member of the PEP or a person known to be a close associate of the PEP;
- 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;
- 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/CTF systems that are in accordance with the recommendations of the FATF.

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 control mechanisms for AML of the Customer and the entity receiving funds;
- obtain approval from the Management Board and MLRO 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 Customer 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, when preventing transactions or Business Relationships carried out with the PEP, the family member of the PEP, or a person known to be a close associate of the PEP, the Company must apply the following measures, with the aim not to onboard any PEPs or persons anyhow related to PEPs:

- obtain clarification and confirmation from the MLRO before deciding if establishing a Business Relationship with such a Customer or continuing the Business Relationship with the Customer is not related to the PEP status;
- take adequate measures to establish the sources of wealth and sources of funds, that are involved or might be involved in the Business Relationship, transaction, or any other action or operation;
- 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, the Company must apply the following measures:

- obtaining additional information on the Customer and on their Beneficial Owner;
- obtaining additional information on the intended nature of the Business Relationship;
- obtaining information on the source of funds and source of wealth of the Customer and their Beneficial Owner;

- obtaining information on the reasons for the intended or performed transactions;
- obtaining the approval of the Management Board and MLRO 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;
- ensuring 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 EEA or in a Third 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/CTF systems that are in accordance with the recommendations of the FATF, the Company must apply the following measures:

- obtaining the approval of the Management Board and MLRO for establishing Business Relationships with the Customer or continuing Business Relationships with them;
- obtaining 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 in a credit institution registered or having its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council are in force;
- the application of CDD measures regarding the Customer or their representative while being at the same place as the Customer or their representative;
- gathering additional information about the Customer and its Beneficial Owner, including identification of all owners of the Customer, including those whose shareholding is no more than 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 case of application of EDD measures, the Company reassesses the Customer's risk profile no later than every six months.

CUSTOMER DUE DILIGENCE MEASURES

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:

- name(s) and surname(s);
- personal identification number;[17]
- citizenship;[18]
- photograph;

[17] in case of a foreigner – date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification), the number and period of validity of the residence permit in the Republic of Lithuania and the place and date of its issuance (applicable to foreigners);
[18] 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.

- signature of the individual[19]

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 of the Republic of Lithuania;
- an identity document of a foreign state;
- a residence permit in the Republic of Lithuania;
- a driving license issued in a state of the European Economic Area in accordance with the requirements laid down in Annex I to Directive 2006/126/EC of the European Parliament and of the Council of 20 December 2006 on driving licenses (recast).

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

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:

- business name or name;
- legal form;
- registration number, if such number has been issued;
- name(s) and surname(s), personal number (in case of a 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;
- head office (address) and address of actual operation.

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 an 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

[19] except for the cases where it is optional in the identity document

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 identification of the Customer'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 has to be in line with the requirements of the Lithuanian Civil Code. The authorisation issued abroad has to be legalized or bear an Apostille. 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.

The identification of the Customer'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):

- name(s) and surname(s);
- personal number;[20]
- citizenship.[21]

[20] in case of a foreigner – date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification), the number and period of validity of the residence permit in the Republic of Lithuania and the place and date of its issuance (applicable to foreigners);
[21] 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.

The Company shall request from the Customer information to 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 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 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[22] or indirect[23] shareholding. Family connections and contractual connections must also be taken into account here;
- who is the natural person in senior management[24], who must be defined as the Beneficial Owner, as a result of execution of the previous two stages has not made it possible for the obliged entity to identify the Beneficial Owner.

When determining and verifying the identity of the Customer registered in Lithuania, the Company does not start a business relationship or carry out a one-time monetary operation or transaction (except for monetary transactions or transactions concluded and/or executed during the course of a business relationship), when information about the Customer-legal entity's beneficiaries under Article 25 of the AML Law is not provided in the Information System of Legal Entities Participants (Lithuanian: JADIS) or when the information about the beneficiaries of a Customer – a legal entity, provided in the procedure established in Article 25 of the AML Law in the Information System of Participants of Legal Entities (JADIS), does not correspond to the information the Company has about the beneficiaries of the same Customers.

For Customers registered outside Lithuania, unless there are public (state) documents proving the ultimate beneficial owners, the Customers' provided 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

[22] **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

[23] **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.

[24] a **member of senior managemen**t 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.).

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, confirmed by the check results in independent source of information.

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.

Use of the Information System of Legal Entities Participants

When identifying a Beneficial Owner, the Company must additionally use the Information System of Legal Entities Participants (JADIS) from which to obtain data on Beneficial Owners of the Customer and shall have the right to use other state information systems and registers in which data on the participants of legal persons are accumulated.

JADIS can be accessed through the Lithuanian State Enterprise Centre of Registers' (SECR) via the relevant application. The application may be submitted:

- electronically through the user self-service system of the Centre of Registers;
- by e-mail info@registrucentras.lt which should be signed by e-signature;
- at the Client Service Offices of the Centre of Registers by submitting its original.

The prepared JADIS excerpts and copies of documents may be:

- downloaded from the self-service of the Centre of Registers (only if the application has been filed through the self-service of the Centre of Registers);
- collected at the Client Service Offices of the Centre of Registers;
- received by post to the address indicated by the client.

Upon the determination of the discrepancy between the information on the Beneficial Owners of the Customer that is a legal person available in JADIS and the information on the Beneficial Owners of the same customer available to them, notify the Customer thereof and propose to provide accurate information on its Beneficial Owners to the data processor of JADIS.

The Company shall not enter into a Business Relationship or execute a transaction (except for monetary operations or transactions concluded and/or executed in the course of a Business Relationship), when

the information on the Beneficial Owners of the Customer that is a legal person is not provided in JADIS or when the information on the Beneficial Owners of the Customer that is a legal person, provided in JADIS, is incorrect.

Identification of Politically Exposed Persons (PEPs)

The Company does not onboard PEPs and applies de-risking policy for PEPs. The Company shall take measures to ascertain whether the Customer, the Shareholder (-s) (Member), Beneficial Owner (-s) of the Customer, the Head (-s) or otherwise authorized representative (-s) of this Customer is not a PEP, their family member[25] or close associate[26] 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. A potential PEP must be additionally screened using international, reliable, and independent search engines, databases, or systems, 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 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 board 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 Lithuanian armed forces, commander of the armed forces and units, chief of defense staff or senior officer of foreign armed forces;

[25] **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.
[26] **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.

- 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 or supervisory body of a municipal 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, and which are considered as large enterprises in terms of the Law on Financial Statements of Entities of the Republic of Lithuania;
- 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 has been a PEP no longer performs important public functions placed upon them, the Company shall, at least within 12 months period, 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 case of the Customer. The Company does not onboard persons having been PEPs or PEP-related persons at periods and/or dates less than 12 months before applying to open an account at the Company.

Identification of the purpose and nature of the business relationship or 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 Firm 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 or an Occasional Transaction 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 to 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.

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 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 Company shall perform regular monitoring and KYC updates on an ongoing basis upon establishment of a Business Relationship. The frequency of the ongoing verifications depends on the Customer's risk profile. The regularity of the checks and updates must be based on the risk profile of the Customer, and the checks must take place at least:

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

- once per quarter 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., retrospective 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 Virtual Currency wallets where the Virtual Currency shall be sent in accordance with the Customer´s order;
- the scoring of Virtual Currency wallets from which the Virtual Currency is received.

If the Customer gives order for transaction which exceeds the threshold established or for transaction to the Virtual Currency 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, Virtual Currency sending each time to new Virtual Currency 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 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 transaction regularly (at least once per week) 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**[27] **and origin**[28] **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 reasonably considers 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.

[27] **the source of the funds** used in the transaction is reason, explanation and basis (legal relationship and its content) why the funds were transferred

[28] **the origin of the funds** used in the transaction is the activity by which the funds were earned or received

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 FCIS thereof within 3 hours.

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

The Company shall use at least the following sources (databases) to verify the Customer´s relation to Sanctions (non-exhaustive list):

- A consolidated list of EU sanctions; the EU Sanctions Map; European Council / Council of the European Union;
- A consolidated list of United Nations sanctions;
- OFAC Sanctions;
- The UK Sanctions List;
- LT FIU List of Legal persons or other organizations without legal person status whose property is legally owned or controlled by the entity to which sanctions apply;
- Lithuanian Ministry of Foreign Affairs – Implementation of International Sanctions.

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

Before establishing a relationship with the customer or concluding a transaction, the Company makes sure that the customer, beneficiary, and/or representative of the customer is not on the list of persons subject to international financial sanctions.

To make sure that transactions are not carried out, and business relations are not maintained or established with persons subject to international financial sanctions, the Company checks the persons subject to international financial sanctions of necessarily at least of both the European Union and the United Nations financial sanctions, lists.
The Company follows compliance with the Law on International Sanctions of the Republic of Lithuania, the resolutions of the Government of the Republic of Lithuania on the implementation of the Law on International Sanctions, the regulations of the European Union on international sanctions, and exceptions to their implementation, and order no. V-273 "Regarding the approval of supervision instructions of the Financial Crimes Investigation Service under the Ministry of Internal Affairs of the Republic of Lithuania in the field of regulation of the proper implementation of international financial sanctions" of the Director of the Financial Crimes Investigation Service of 20 October 2016.

The Company also follows the compliance requirements in accordance with the resolutions, instructions, and other sanctions-related material issued by the Bank of Lithuania (the BOL), namely, the following:

- Instructions for the Financial Market Participants regarding the Implementation of International Sanctions, approved by Resolution No. 03-98 of the Board of the Bank of Lithuania of 30.05.2023;
- Information notices of the BOL, related to implementation and updates of the regional and international sanctions;
- Expectation Letters (so-called Dear CEO letters) and Recommendations of the BOL, issued in the years 2021-2023, etc.

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 or trademark, registry code or registration date, and for a natural person, their name and personal identification 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.).

If the Employee has doubts that a person is a subject of Sanctions, the Employee shall immediately notify the MLRO or the Management Board. In this case the MLRO or the Management Board shall decide whether to ask or acquire additional data from the person or notify the FCIS 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 Business Relationship, perform a transaction, or an act with them, whether the information is from a credible and independent source and assess the answer.

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 about the identification of the subject of Sanctions, of the doubt thereof and of the measures taken.

The MLRO or the Management Board shall refuse to conclude a transaction or proceeding, take measures provided for in the act on the imposition or implementation of the Sanctions, and immediately notify the FCIS 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 what is implemented against the person to ensure legal and proper application of measures.

REFUSAL TO THE TRANSACTION OR BUSINESS RELATIONSHIP AND THEIR TERMINATION

The Company is prohibited to establish 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 which 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”).

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 no later than within one month after the termination and as a whole to an account opened in a credit institution which is registered or whose place of business is in a contracting state of the European Economic Area or in a country where requirements equal to those established in the relevant directives of the European Parliament and of the Council are applied. 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.

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 FCIS 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 minimum characteristics of suspicious transactions are provided in the guidelines made by the FCIS (one of the annexes of these Guidelines).

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 abovementioned 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 no 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).

Reporting obligation regarding specific types of transactions

The Company through its MLRO must send information to the FCIS not later than within 7 working days after the identification of Virtual Currency exchange transactions or transactions in Virtual Currency, if the daily value of such transaction(s) is equal to or exceeds EUR 15,000 or the equivalent amount in foreign or Virtual Currency, regardless of whether the transaction is concluded in one or more related monetary transactions.

In case specified above information submitted to the FCIS shall include:

- 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 FCIS 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 FCIS, a plan to submit such a report or the occurrence of reporting as well as about a precept made by the FCIS or about the commencement of criminal proceedings.

TRAINING OBLIGATION

The Company 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 (the **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 Company on ensuring the suitability of Relevant Persons, the Company makes sure that such persons receive appropriate training and information on an ongoing basis to be able to fulfil the Company's obligations in compliance with the applicable legislation. It is ensured through training that such persons are knowledgeable within the area of AML/CTF 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 Company's risk assessment, the Company'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/CTF 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 Company'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 Company's Employees and Relevant Person engaged.
- scope: review of applicable rules and regulations, the Company'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, the 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.

COLLECTION AND STORING OF DATA, LOGBOOKS

The Company 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
- the each transaction date or period and a description of the contents of the transaction, including the transaction amount, the currency and the account number or another identifier (incl. hash of transactions in Virtual Currency and Virtual Currency wallets related to transaction);
- information serving as the basis for the reporting obligations specified in the Guidelines;
- data of suspicious or unusual transactions or circumstances of which the FCIS 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).

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 8 years after the expiry of the Business Relationship or the completion transaction. The data related to the performance of the reporting obligation must be retained for 8 years after the performance of the reporting obligation. The correspondence of a Business Relationship with the Customer must be retained for 8 years 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 the FCIS or, pursuant to legislation, other 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.

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 customers who perform transaction(s) in Virtual Currency regardless circumstance if transaction(s) are performed occasionally or in the course of Business Relationship;
- logbook of Monetary Operations or transactions performed between the Customer and the Company prior to when the Company is obliged to apply CDD measures;
- logbook of reports[29] and suspicious monetary transactions and transactions;
- 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 Customers who perform transactions in Virtual Currency shall include the following:

- 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 (date of birth of an foreigner Customer), citizenship; personal code, if such a code is provided;
- in case of Virtual Currency transactions or transactions, it is not objectively possible to identify the payee, other information enabling the Virtual Currency Address to be linked to the identity of the Virtual Currency owner: Internet Protocol (IP) address, e-mail address, etc.;
- Virtual Currency Address(es) related to transaction and transaction's hash(es);

[29] as described in the relevant chapter of these Guidelines.

- transaction method: deposit or withdrawal of Virtual Currency, Virtual Currency is exchanged to money or vice versa, Virtual Currency exchanged to other Virtual Currency, Virtual Currency exchange transaction was mediated (p2p exchange);

Registration logbook of Monetary Operations or transactions performed between the Customer and the Company prior when the Company is obliged to apply CDD measures shall include the following:

- 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 (date of birth of an foreigner Customer), citizenship; personal code, if such a code is provided;
- 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.);
- transaction method: Virtual Currency is exchanged to money or vice versa, the Customer made prepayment for buying Virtual Currency, etc.

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 (date of birth of an foreigner Customer), citizenship; personal code, if such a code is provided;
- the criterion approved by the Ministry of the Interior of the Republic of Lithuania, according to which it is recognized that the Customer's monetary transaction or transaction is considered suspicious, the transaction or transaction complies with;
- 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 personal ID number of a natural person (in case of a foreigner: date of birth, where available, personal ID number or any other unique sequence of symbol assigned to relevant individual for personal identification), and in case of legal entity, title, legal form, registered address, and registration number, if such has been assigned;
- contact details of the Customer: phone number(s), e-mail address(es), contact person(s), their phone numbers, email addresses, etc.;
- 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 (date of birth of an foreigner Customer), citizenship; personal code, if such a code is provided;
- 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 case of Virtual Currency transactions or transactions, it is not objectively possible to identify the payee, other information enabling the Virtual Currency address to be linked to the identity of the Virtual Currency owner: Internet Protocol (IP) address, e-mail address, etc.;
- in case of Virtual Currency transactions Virtual Currency Address(es) related to transaction and transaction's 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: date of birth, where available, personal ID number or any other unique sequence of symbol assigned to relevant individual for personal identification), and in case of legal entity, title, legal form, registered address, and registration number, if such has been assigned;
- reasons for termination of transactions or Business Relations pertaining to breaches of procedure of prevention of Money Laundering and/or Terrorist Financing.

Procedure for keeping and administration of registration logbooks

The storage of log data shall be completed and kept on an electronic medium by the Management Board member, if he/she is on a business trip, or is otherwise unavailable for other valid reasons, another Employee, as indicated in the special order of the director, setting out the scope of duties and responsibilities assigned to an individual acting as a substitute.

The Management Board shall appoint an Employee charged with a duty to ensure protection of the data included in the registration logbooks, and processed in an electronic medium, from unauthorized deletion, alteration, or use by the third unauthorized parties.

Details shall be stored using software allowing for export of details stored to Microsoft Office Excel, Word, or equivalent open-code software, without damaging integrity of the details.

Keeping of the registration logbooks shall be verified by a Management Board, if he/she is on a business trip, or is otherwise unavailable for other valid reasons, another responsible Employee appointed by the Company, as indicated in the special order of the director, setting out the scope of duties and responsibilities assigned to an individual acting as a substitute.

The Employees of the Company shall be prohibited to inform, or otherwise let know, any Customer or other individuals that information on the Monetary Operations taking place, or transactions conducted by a Customer, or resulting investigation is communicated to the FCIS.

INTERNAL CONTROL OF EXECUTION OF THE GUIDELINES

The performance of the Guidelines shall be internally controlled by the Management Board, or the Employee appointed by the Management Board for performing relevant functions (hereinafter in this chapter – **Internal Control Officer**). The Internal Control Officer must have the required competency, tools, and access to the relevant information in all structural units of the Company.

The Internal Control Officer 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 refuse to the transaction or business relationship and their termination;
- the Company´s reporting obligation to the FCIS;
- the Company´s training obligation regarding the AML/CTF requirements;
- the Company´s obligation for collection and preservation of data.

The exact measures for performing internal control shall be determined by the Internal Control Officer and must correspond to the Company's size and their nature, scope and level of complexity of the activities and services provided. The Internal Control Offices must consider at least examination fields specified above. The internal control measures shall be performed at the time determined by the Internal Control Officer 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 within 8 years. Only Management Board members and Internal Control Officer may have access to the Internal Control Data. Internal Control Officer may provide access to the Internal Control Data to other Employees or third parties (e. g. advisors, auditors, etc.) only with prior consent of Management Board. The persons 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 understandable connect this to other relevant data.

The Internal Control Officer 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 resolution regarding it. The Internal Control Officer 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 by the European Commission of the results of an EU-wide money laundering and terrorist financing risk assessment (available on the European Commission's website http://ec.europa.eu);
- after the publication of the results of the National Money Laundering and Terrorist Financing Risk Assessment (published in the section “National Money Laundering and Terrorist Financing Risk Assessment” of the section “Prevention of Money Laundering” of the website www.fntt.lt);
- upon receipt of an instruction from the FCIS to strengthen the applicable internal control procedures;
- in the event of significant events or changes in the management and operations of the depository virtual currency money operator and the virtual currency exchange operator.

Risk assessment and risk appetite

The target of the implementation of internal control measures for Company’s compliance with established risk assessment policy (incl. established risk appetite) is examination of the following circumstances:

- Company establishes and uses risk-based approach when providing services to the Customers (e.g., CDD measures implemented in accordance with risk level);
- Company determined factors which affecting the arise of ML/TF risks and determined factors are relevant;
- Company determined and assessed ML/TF of all services which Company provides;
- Company composed the risk profile of the Customer prior the performing transactions or creating business relationship;
- Company updates risk profile of the Customer on regular basis;
- Company follows established risk appetite;
- Company keeps records of all incidents in accordance with established risk assessment policy;
- risk assessment policy was reviewed during the last year and there is no information that MLRO had required earlier review.

Customer due diligence measures implementation

The target of the implementation of internal control measures for Company's compliance with CDD measures implementation is an examination of the following circumstances:

- the Company apply CDD measures prescribed by the Guidelines to all relevant Customers;
- the Company collects proper documents and information when applying CDD measures;
- the Company properly verifies data and documents collected when applying CDD measures;
- the Company applies the relevant level of CDD measures (e. g. EDD measures, etc.);
- the Company applies proper EDD measures to specific Customers (e. g. high-risk country, etc.);
- the Company performs Customers´ identification in accordance with established procedure;
- the Company properly identifies Customers´ representative(s);
- the Company properly identifies Customers´ beneficial owners;
- the Company properly identifies Customers´ likelihood to PEP status;
- the Company properly identifies purpose and nature of business relationship or transaction;
- the Company properly monitors business relationships with Customers.

Implementation of Sanctions

The target of the implementation of internal control measures for Company's compliance with implementation of Sanctions is an examination of the following circumstances:

- the Company applies procedure for identification of a subject of Sanctions or transaction violating Sanctions;
- the Company performs actions if identifies a subject of Sanctions or transaction violating Sanctions.

Obligation to refusal of transaction or business relationship and their termination

The target of the implementation of internal control measures for Company's compliance with obligation to refuse the transaction or business relationship and their termination is an examination of the following circumstances:

- the Company refuses transaction or business relationship if it´s obligatory in accordance with the Guidelines;
- the Company refuses or terminates transaction or business relationship if it´s obligatory in accordance with the Guidelines.

Reporting obligation

The target of the implementation of internal control measures for Company's compliance with reporting obligation is an examination of the following circumstances:

- the Company sends reports and information to the FCIS, if it's required by the Guidelines (incl. relevant FCIS's guidelines);
- the reports sent to FCIS are filled in accordance with the FCIS's guidelines.

Training obligation

The target of the implementation of internal control measures for Company's compliance with training obligation in AML/CTF field is an examination of the following circumstances:

- all Employees (incl. MLRO and Management Board members) have relevant training;
- each Employee (incl. MLRO and Management Board members) has been training for the last 360 days.

Obligation of collection and preservation of data

The target of the implementation of internal control measures for Company's compliance with obligation of collection and preservation of data is an examination of the following circumstances:

- all data which shall be saved in accordance with the Guidelines (hereinafter in this chapter – the **Saved Data**) have been properly saved in chronological order with format, which allows to analyze this and understandable connect the Saved Data to other relevant data;

- only Employees (incl. MLRO and Management Board members) or authorized third parties have access to the Saved Data;
- all relevant logbooks are kept in accordance with the Guidelines;
- the Saved Data in electronic format has backup;
- the Saved Data in other formats (e. g. on paper) has backup in electronic format;
- the Saved Data is irrevocably deleted in accordance with the Guidelines.

VERSION CONTROL TABLE

Version	Approval Date	Document Author	Approving Body	Remarks
1.0	20.12.2021	Lawyers	Director Dejan Jursa	
2.0	22.05.2023	AML Compliance Officer Agnė Bimbirytė	Director Dejan Jursa	
3.0	11.10.2024	AML Compliance Officer Agnė Bimbirytė	Director Kai Werner Schwab	
4.0	30.10.2024	AML Compliance Officer Agnė Bimbirytė	Director Kai Werner Schwab	