ANTI-MONEY LAUNDERING AND COUNTER TERRORIST FINANCING COMPLIANCE POLICY

BT Exchange (LT) UAB

Document History

Version	Approval Date	Author	Change Status	Approved by
2.0	05.06.2024	BT EXCHANGE (LT)UAB	Second issue	Jad Abdel Rahman

CONTENT

BT Exchange (LT) UAB (hereinafter – the "**Company**") is a virtual currency exchange and depository wallet operator, acting according to the laws of the Republic of Lithuania. The Company is committed to conducting business operations in a transparent and open manner consistent with its regulatory obligations.

1. TERMS AND DEFINITIONS

1.1. "**Money laundering**" or "**ML**" means the doing of any act which constitutes an offence of money laundering under the Criminal Code of the Republic of Lithuania and is defined in the Law on the

Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania. The criminal acts cover all procedures that seek to change the identity of illegally obtained funds, arising from drug dealing, terrorist activities or any other crime in order to give impression that such money originated from legitimate or legal sources. Money laundering is the participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities such as, for example, fraud, corruption, organized crime, or terrorism etc. Predicate offences for money laundering are defined by the Criminal Code of the Republic of Lithuania.

1.2. "**Terrorist financing**" or "**TF**" means the provision of funds, directly or indirectly, with the intention that they should be used or in knowledge that they are to be used in order to carry out any of the offences within the meaning of Articles 1-4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (as amended by Framework Decision 2008/919/JHA of 28 November 2008) and falling under Articles 250, 250^1 – 250^6 of the Criminal Code of the Republic of Lithuania.

1.3. "**Company**" means **BT EXCHANGE (LT) UAB**. The term "Company" when used in these Procedures also refers to the management bodies of the Company and the members of such bodies as well as the employees of the Company.

1.4. "**Employee of the Company**" or "**Employee**" means any natural person who is employed by the Company on the basis of employment agreement or other agreement. The term "Employee" when used in these Procedures also refers to the management bodies of the Company and the members of such bodies, unless the context requires otherwise.

1.5. "**Client**" means a person that uses services provided by the Company.

1.6. "**Beneficial owner**" means a natural person who ultimately owns or controls the Client or a natural person on whose behalf a Transaction is being conducted or the Monetary operations is being executed. The Beneficial owner is:

(1) as regards corporate entities:

a. a natural person who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings (a percentage of 25% plus one share shall be deemed sufficient to meet this criterion), save a company listed on a regulated market that is subject to disclosure requirements consistent with the legislation of the European Union or subject to equivalent international standards;

b. a natural person who otherwise exercises control over the management of a corporate entity;

(2) as regards legal entity which administers and distributes funds:

a. a natural person who is the beneficial owner of 25% or more of the property of a legal entity (where the future beneficial owners have already been determined);

b. where the individuals that benefit from this legal entity have not yet been determined, the class of persons in whose main interest the legal entity is set up or operates;

c. a natural person who exercises control over 25% or more of the property of the legal entity.

1.7. "**Business relationship**" means a business, professional or commercial relationship of the Company with a Client that is expected, at the time when entering in such relationship, to have an element ofduration.

1.8. "**Transaction**" means a contractual arrangement between the Company and the Client on the provision of the virtual currency services.

1.9. "**Monetary operation**" means any payment, transfer or receipt of funds executed by the Company under the instructions of a Client, save the payments to state and municipal institutions, other budgetary institutions, the Bank of Lithuania, state or municipal funds, diplomatic missions or consular posts of foreign countries or settlement with these institutions.

1.10. "**Suspicious Monetary operation or Transaction**" means a Monetary operation or Transaction which relates to either the funds derived from the illegal activities or the funds obtained in the course of the illegal activities or the terrorist financing and which meets at least one of the criteria established by the Order of the Director of the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania No V-240 of 5 December 2014 as described in details in Section 7 below.

1.11. "**Politically exposed natural person**" or "**PEP**" means a natural person who is or has been entrusted with prominent public functions and immediate family members or persons known to be close associatesof such person. A person is considered to be a PEP for a period of 1 year after ceasing to be entrusted with the Prominent public functions.

1.12. "**Prominent public functions**" means functions within the Lithuanian, European Union, international or foreign public authorities:

(1) 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;
(2) a member of the parliament;
(3) a member of the Supreme Court, the Constitutional Court or any other supreme judicial authorities whose decisions are not subject to appeal;
(4) a mayor of the municipality, a head of the municipal administration;
(5) a member of the management body of the supreme institution of state audit or control, or a chair, deputy chair or a member of the board of the central bank;
(6) an ambassador, a *chargé d'affaires ad interim*, a special envoy and a minister plenipotentiary or a high-ranking military officer;
(7) 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;
(8) 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 of the Republic of Lithuania on Financial Statements of Entities;
(9) a director, a deputy director or a member of the management or supervisory body of an international intergovernmental organisation;
(10) a leader, a deputy leader or a member of the management body of a political party.

1.13. "**Close associate**" means a natural person who:
(1) participates in the same legal entity or maintains other business relationships with a person who performs or previously performed the prominent public functions;
(2) is the sole owner of the legal entity set up or operating de facto with the aim of acquiring property or another personal benefit for a person who performs or previously performed the prominent public functions.

1.14. "**Close family member**" means spouse, person in registered partnership (cohabitant), parent, brother, sister, child and child's spouse or child's cohabitant.

1.15. "**Financial institution**" means the credit institutions and financial undertakings as defined in the Law of the Republic of Lithuania on Financial Institutions, payment institutions as defined in the Law of the Republic of Lithuania on Payment Institutions, electronic money institutions as defined in the Law of the Republic of Lithuania on Electronic Money and Electronic Money Institutions, operators of currency exchange offices as defined in the Law of the Republic of Lithuania on Currency Exchange Operators, operators of crowdfunding platforms as defined in the Law of the Republic of Lithuania on Crowdfunding, operators of peer-to-peer lending platforms as defined in the Law of the Republic of Lithuania on Consumer Credit and the Law of the Republic of Lithuania on Credit Relating to Immovable Property, insurance undertakings engaged in life insurance activities and insurance brokerage firms engaged in insurance mediation activities relating to life insurance as defined in the Law of the Republic of Lithuania on Insurance as well as investment companies with variable capital and collective investment undertakings intended for informed investors and management companies managing only those undertakings; branches of these foreign financial institutions set up in the Republic of Lithuania as well as electronic money institutions and payment institutions whose registered office is in another European Union Member State providing services in the Republic of Lithuania through agents, natural or legal persons.

1.16. "**European Union Member State**" or "**EU Member State**" means a state which is a Member State of the European Union ("**EU**") or a state of the European Economic Area ("**EEA**").

1.17. "**Third party**" means a Financial institution or another entity as defined in the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania as well as a financial institution or another entity registered in another EEA Member State or a state which is not a EEA Member State (third country), who meets the following requirements:
(1) they are subject to mandatory professional registration, recognized by law;
(2) they are registered in a EU Member State or in a third country which applies requirements that are equivalent to the EU identification requirements and record keeping requirements in respect of Clients and Beneficial owners, and which is monitored by the competent authorities in terms of the compliance with the said requirements.

1.18. "**Other than FATF country**" means (i) a country that is not a member of the Financial Action Task Force ("FATF") on Money Laundering or of an international organization with an observer status at

FATF that participates in the efforts to combat money laundering and terrorist financing and (ii) considered to be High-risk and non-cooperative jurisdiction. The list of the countries other than FATF countries is provided under the following link: http://www.fatf-gafi.org/countries/#high-risk.

1.19. "**Target territory**" means a foreign state or zone as specified in the Law on Corporate Income Tax of the Republic of Lithuania. The list of the target territories is attached to these Procedures as Annex Four.

1.20. "**Financial intelligence unit**" or "**FIU**" means the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania.

1.21. "**Money laundering reporting officer**" or "**Officer**" means an employee of the Company who is appointed by the managing director of the Company as the officer responsible for the ML and TF prevention in the Company.

1.22. "**Procedures**" means these procedures on the prevention of money laundering and terrorist financing and all its annexes as may be further amended from time to time.

1.23. **"Virtual currencies"** shall mean a digital representation of value that does not possess a legal status of currency or money, that is not issued or guaranteed by a central bank or any other public authority, is not necessarily attached to a currency, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

1.24. **"Virtual currency address"** shall mean an 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.

1.25. "**Register** " means all and any electronic register which the Company keeps

2. ROLES AND RESPONSIBILITIES

2.1. **The Board** has a critical oversight role - as the senior-most management of the company, they should approve and oversee policies for risk, risk management and compliance. The Board also should have a clear understanding of the ML risks, including timely, complete, and accurate information related to the risk assessment to make informed decisions. Along with the General manager, the Board should appoint a qualified AML Officer with overall responsibility for the AML function and provide this senior-level officer with sufficient authority that when issues are raised they get the appropriate attention from the Board, the General manager and the business lines. The board will ensure that all employees are aware of the person who has been assigned the duties of the AML Officer to whom they report, any information concerning transactions and activities for which they have knowledge or suspicion that might be related to ML and TF. The Board is responsible for the overall AML/CTF compliance policy of the Company and ensuring adequate resources are provided for the proper training of staff and the implementing of risk systems. The Board will receive and consider quarterly compliance reports presented by the AML Officer.

2.2. **The General Manager** will receive and consider the monthly compliance reports sent by the AML Officer and authorize changes based on the recommendations if required. General Manager will also receive reports on particularly significant changes that may present risk to the organization. Assistance may be given to the AML Officer in the preparation of the AML program.

2.3. **The Compliance Officer (AML Officer)** is responsible for managing compliance risks, developing risk management and company's policies and procedures, and monitoring compliance issues. The AML Officer is responsible for reporting significant changes that may present high ML/TF risks to the Company. The AML Officer prepares monthly and quarterly reports for consideration to the General Manager and the Board and conducts risk assessments of compliance systems, develops regular random analysis. The AML Officer establishes and implements the risk scoring matrix following regulatory guidance and for review and approval by the General Manager.

2.4. **The MLR Officer (MLRO)** is responsible for Transaction monitoring, receiving internal disclosures and making reports to the Financial Crime Investigation Service (FCIS). First point of contact for all compliance issues from staff. MLRO undertakes regular random analysis of transactions including assessment of documentary evidence provided by Clients and prepares any necessary amendments to the Policy in line with risk assessment. MLRO ensures everyone is periodically informed of any changes in anti-money laundering and anti-terrorist financing legislation, policies and procedures, as well as current developments and changes in money laundering or terrorist activity financing schemes particular to their jobs, constructing AML/CTF-related content for staff training programs. Independently from front office staff, MLRO reviews Client identification information to ensure that all the necessary information has been obtained.

2.5. **Other staff members** are responsible familiarize with this Policy, other internal procedures related to their job role and understanding responsibilities. Ensure AML/CTF procedures are adhered to. Ensure that all suspicious activity is reported to the AML Officer.

3. PROCEDURES TO FOLLOW

3.1. While complying with the legal procedures and implementing the ML/TF prevention measures, Employees depending on their position and functions within the Company must comply with the following procedures described in details further in these Procedures:

(1) Procedure of AML trainings;
(2) Procedure of reporting;
(3) Procedure of identification of customers;
(4) Procedure of monitoring;
(5) Procedure of business wide risk assessment;
(6) Procedure of implementation of international sanctions;

4. KYC PROCEDURES (CLIENT DUE DILIGENCE)

4.1. Client Due Diligence ("**due diligence"** or **"CDD**") process must comply with procedures as detailed herein. These include the identification of the Client, ML/TF risk assessment, assessment of the financial position of the Client, validity of identity and the source of funds.

4.2. The following procedures which constitute the ML/TF prevention measures shall be carried out in order

to perform customer due diligence **prior to establishing a business relationship**:

(1) identification of persons who apply to the Company as the potential Clients;
(2) verification if the potential Clients acts as a principal; if the potential Clients is represented by other person (agent), the identification and verification of the representative (agent) applies as well;
(3) identification and verification of the identity of the Beneficial owner, if applicable;
(4) identification of the identity of the Client's director (Full name, date of birth or personal code, nationality), if applicable;
(5) obtaining information on the Client's management structure and the nature of its activity, if applicable;
(6) obtaining information on purpose and intended nature of the relationship with the Company; the above steps are essential prior to initiation of a Business relationship with the potential Client and **after the Client is engaged in the Business relationship**, the following ML/TF prevention measure must be taken:

(7) ongoing monitoring of the Business relationship with the Client and the Monetary operations and Transactions of the Client.

4.3. The Client can be turned away before a Business relationship is formed, during the due diligence process or the stages following acceptance of a Business relationship.

5. IDENTIFICATION OF THE CLIENTS, THE BENEFICIAL OWNERS AND THE REPRESENTATIVES OF THE CLIENTS (WHERE APPLICABLE)

5.1. The Company requires a good working knowledge of the Client's activities in order to provide an effective service, including evidence of their identity. The Company **needs to identify the Clients, their Beneficial owners (where applicable) and the representatives (where applicable) in the following circumstances**:

(1) prior to establishing business relationship. The creation of a deposit wallet of virtual currencies is not a business relationship if no more than one transaction, operation, deposit or withdrawal has taken place in that wallet within six months and the amount is less than EUR 1 000 or currency/ virtual currency equivalent;
(2) before:
   a. executing occasional virtual currency exchange transactions or operations in virtual currency with funds equal to or above EUR 1,000 or currency/virtual currency equivalent;
   b. occasional depositing or withdrawing of virtual currency amounting to or above EUR 1,000 or currency/virtual currency equivalent;;
   c. transaction is carried out in one or more interrelated transactions (the value of the virtual currency being determined at the time of the monetary transaction or operation) unless the customer and beneficial owner have already been identified.
   d. when executing and accepting money transfers in compliance with the provisions of Regulation (EU) No 847/2015 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006;
(3) when there are doubts about the veracity or adequacy of previously obtained identification data of the Client and/or the Beneficial owner and/or the representative of the Client (where applicable);
(4) in any other case when there are suspicions that the act of ML or TF is, was or will be performed.

5.2. The identification evidence must be obtained before the provision of any services to a prospective Client or an established Client – if sufficient evidence cannot be obtained the Company must not proceed with the business. The more detailed identification requirements are provided in Annex Two to these procedures.

6. IDENTIFICATION METHODS

6.1. Clients may be identified by face-to-face contact, or using non-face-to-face identification methods. This also applies to those cases where the Client, either natural or legal person, is represented by another person.

6.2. When identifying Clients by face-to-face contact, the Client must provide an original personal identification document – for natural persons; or the registration and/or other corporate documents – for legal persons. More detailed requirements on face-to-face identification are provided in Annex Two.

6.3. The non-face-to-face identification can be executed:

6.3.1. When information about Client's identity is certified by his qualified electronic signature which complies with the requirements of Regulation (EU) No 910/2014.

6.3.2. When information about Client's identity is confirmed by electronic identification means issued in the European Union and functioning under electronic identification schemes with high or substantial assurance level under Regulation (EU) No 910/2014.

6.3.3. Using electronic means, allowing direct view transmission, in one of the following ways:

(a) identity document issued by the government body is captured using video-streaming and identity is confirmed using at least an advanced electronic signature, meeting the requirements referred to in Article 26 of Regulation (EU) No 910/2014;

(b) Client's facial image and original identity document issued by the government body are captured using video-streaming.

6.3.4. Using the Third party information on the Client or the Beneficial owner;

6.3.5. Before commencing the use of the services of the Company, a payment order is made to the payment account of the above institution from the account held on behalf of the Client in the credit institution which is registered in the EU Member State or in a third country which applies the requirements equivalent to those specified in the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and which is monitored by competent authorities as to the compliance with such requirements, and a paper copy of the identification document, which is approved in the manner prescribed by legal acts of the Republic of Lithuania, is submitted.

6.4. The more detailed information and technical requirements for non-face-to-face identification methods are provided in Annex Three.

7. RISK ASSESSMENT

7.1. An important aspect of the due diligence process is the assessment of the risks involved and the acceptability of a prospective Client. Before agreeing to provide a service to a prospective Client, an assessment of the risks involved should be completed. This involves assessing the acceptability as a Client and the risk associated with the particular services requested by the Client. This on-going evaluation is necessary to consider relevant issues before deciding as to whether the required services should be provided.

7.2. When entering into the Business relationship with the Client, the ML/TF risk is assessed on the basis of the documentation and information obtained from a prospective Client. **Special attention must be given to the behavior of and the verbal communication with a prospective Client as well as the criteria of the High Risk Clients and Low Risk Clients as listed in Sections 9 and 10 below**. When assessing the ML/TF risk the aim is to establish and assess the following circumstances:

(1) **type of the Client**, i.e. whether a prospective Client meets the profile of the typical client of the Company; if not, the additional clarification and/or documentation must be requested from the Client seeking to establish if there is a high ML/TF risk; the special attention is given to the following circumstances which may increase the ML/TF risk:

a. if the Client is a PEP;

b. where the prospective Client is a non-profit institution (**"NPI"**);

c. other circumstances indicated in these Procedures;

(2) **commercial relationships**, i.e. assessing if the behaviour of a prospective Client reveals that the

aims and duration of the relationship expected by a prospective Client may considerably differ from what is inherent to the profile of the typical Client of the Company; if yes, the additional clarification and/or documentation must be requested from the Client seeking to establish if there is a high ML/TF risk; in addition it needs to be established if the Client acts as a principal or is represented by the third person (agent);

(3) **product**, i.e. assessing if the virtual currency exchange and wallet services in which a prospective Client is interested correspond the nature of the business and the Transaction profile of such prospective Client; if not, the additional clarification and/or documentation must be requested from the Client seeking to establish if there is a high ML/TF risk; attention should be drawn where the Client or the potential Client is to transact in new or developing technologies which may give rise to a threat of ML/TF or the use of Monetary operations or Transactions that might favour anonymity;

(4) **territory**, i.e. assessing where the main place of interests of a prospective Client is situated, e.g. where the Client is living/incorporated or where the place of the main business activity of the Client is situated or where the main part of the customers of the Client comes from; it is important to establish if such main place of interests of the Client is situated in the country other than FATF country or in the Target territory; in such event the Client has to be considered as a high risk client.

7.3. The following circumstances shall indicate a high risk and accordingly trigger high risk due diligence level:

(1) a prospective Client starts to expresses his interest in the topics related to ML/TF;

(2) a prospective Client is reluctant to perform the actions necessary for identification and to provide information related to the Client and its financial activity;

(3) a prospective Client refuses to provide documents or information requested by the Employee or non-face-to-face identification measures for the identification purposes, especially information/documentation evidencing the financial activity of the Client;

(4) the doubts regarding the correctness or authenticity of the documents or information provided by a prospective Client arises;

(5) a prospective Client is not able to answer the questions provided by the Employee or by non-face-to-face identification measures and related to the financial activity of the potential Client, the nature and the aims of such activity;

(6) a prospective Client is unusually stressed and nervous during the verbal communication with the Employee, especially when asked the questions related to the financial activity of a prospective Client.

7.4. The Officer has to assess the above circumstances, indicated in Point 7.2 and 7.3 above, and decide whether to **refuse accepting the Business relationship with such potential Client** or, if decided to further proceed with the due diligence procedure, **the enhanced due diligence has to be applied**.

7.5. After the risk assessment is performed the Client is assigned to one of three categories according to its risk profile:

(1) **Average Risk Clients** who do not qualify as the High Risk Clients or Low Risk Clients – the standard due diligence and ML/TF prevention measures apply;

(2) **High Risk Clients** who are defined in Section 9 below – the enhanced due diligence and ML/TF prevention measures apply;

(3) **Low Risk Clients** who are defined in Section 10 below – the simplified due diligence and ML/TF prevention measures may apply.

7.6. The profile of the Client is reviewed periodically (at least once a year) reflecting the changes in the Business relationship and behavior of the Client as well as based on the results of the ongoing monitoring of the Client. Thus, the risk profile and, accordingly, the ML/TF prevention measures applied with respect of the Client may change from time to time.

7.7. The Company must ensure that **all risk assessment documentation as well as the results of the risk assessment and all changes to the risk profile of the Client are available in the Company's records (i.e. data base)** and may be made available for the future needs or if required by the relevant authorities.

8. ADDITIONAL SOURCES

8.1. In addition to the information and documentation provided by or on behalf of the Client and obtained from the Third parties (where relevant), the Company has to check the below sources if the provided information is correct or to establish the missing information regarding the Client:

(1) SDN list. List of specially designated nationals and blocked persons. SDN list is a publication of OFAC which lists individuals and organizations with whom United States citizens and permanent residents are prohibited from doing business. https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

(2) EU sanctions list. Consolidated list, containing the names and identification details of all persons, groups and entities targeted by financial restrictions. https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-%09entities-subject-to-eu-financial-sanctions?locale=en

8.2. The sources which the Company applies with regard to the particular Clients may differ depending on the circumstances of each particular case. The Company must ensure that **all results of such searches are available in the Company's records** and may be made available for the future needs or if required by the relevant authorities.

8.3. The requirement to double check the provided information by the Client may not be followed when the Client is the Financial institution.

9. ENHANCED DUE DILIGENCE PROCEDURES

The Company applies the enhanced due diligence procedures in the following instances:

9.1. High Risk Clients

9.1.1. All High Risk Clients and beneficial owner's must be subject to the application of enhanced due diligence measures. For instance, PEPs and the Clients from the high risk territories are considered to pose a higher risk of ML/TF and automatically require the application of enhanced due diligence and ongoing monitoring.

9.1.2. High Risk Clients are also those **Clients who are assigned to this category after the risk assessment or due to the results of the ongoing monitoring**, e.g. the High Risk Clients are as follows (a non-exhaustive list):

(a) those who do not correspond to the profile of the typical Client of the Company significantly and after carrying an additional investigation the Employee decided that the Client or its activityraises high ML/TF risk;

(b) those whose behavior during the due diligence procedure was suspicious and, therefore, reported to the Officer (Section 7 above) who after carrying an additional investigation decided to proceed further with the enhanced due diligence procedure;

(c) whose commercial relationship or behavior during the due diligence procedure were unusual and after carrying an additional investigation it is decided that the Client or its activity raises high ML/TF risk;

(d) the Client performs non-cash transfer operations on the request of persons not related to the main activity of the Client;

(e) the Client is from a high-risk third country identified by the European Commision.

(f) the permanent place of residence of the Client – natural person (where applicable) is a territory other than FATF country;

(g) The Client is engaged in high-risk activities;

(h) The Client s regular business activities involve large number of cash transactions and payments;

(i) suspected terrorism;

(j) the Client – legal person or another organization is registered in a Target territory;

(k) the main place of the interests of the Client is situated in the country other than FATF country or in the Target territory;

(l) the checks in the additional sources as listed in Section 8above reveals that the data of the Client, its representative (where applicable) or the Beneficial owner conform to the data of the persons associated with the ML/TF as specified in the respective lists of the Republic of Lithuania, EU, FATF or the United Nations;

(m) the checks in the additional sources as listed in Section 7 above reveals that the data of the Client, its representative or the Beneficial owner (where applicable) conform to the data of the persons under the financial sanctions in accordance with the Law on Implementation of Economic and other International Sanctions of the Republic of Lithuania;
(n) the unusual behaviour of the Client is established that does not correspond to the ordinary course of activities of the Client (e.g. increasing amounts of payments, especially to the payees or for the goods or services that do not correspond the declared activity of the Client);
(o) those who were assigned to the category of the High Risk Client due to other reasons that raises high ML/TF risk of the Client.

9.2. Politically Exposed Persons

9.2.1. The identification and risk assessment process (Annex Two to these Procedures) or the ongoing monitoring (Section 13 of these Procedures) may reveal the Client or the Beneficial owner (where applicable) to be a PEP as defined in Section 1 of these Procedure. If it is established that the Client or the beneficial owner is a **PEP** then:
(a) this must be notified to the Officer who verifies the information and documentation obtained as well as the additional sources (if needed) and decides whether to refuse (terminate) the Business relationship with such Client or to apply to the authorized senior management of the Company for the approval to establish (continue) a Business relationship with such Client;
(b) the appropriate measures must be taken to establish the source of wealth and funds related to the Business relationship, Monetary operation or Transaction;
(c) the enhanced ongoing monitoring of the Business relationship with the PEP must apply to ensure that the source of wealth and funds that are involved in the PEP's personal/business Monetary operations and Transactions are legitimate.

9.2.2. An individual is considered as PEP for a period of 1 year after ceasing to be entrusted with the Prominent public functions.

9.3. Enhanced Due Diligence Measures

9.3.1. In all of the above instances and apart from normal due diligence procedures, at least one of the following additional measures must be taken:
(a) the additional data, documents or information have to be used to establish the Client's identity;
(b) the additional data, documents or information have to be used to establish the beneficial owner's identity;
(c) obtaining the approval of a senior manager for establishing business relationships with these customers or continuing business relationships with them;
(d) the supplementary measures have to be undertaken to verify or certify the submitted documents or the confirmatory certification issued by other financial institution has to be required;
(e) ensuring that the first payment is carried out through an account held by the Client in his name with a credit institution authorized in the EEA Member State or the third country which imposes equivalent requirements to those laid down in the laws of the Republic of Lithuania.
(f) conducting enhanced monitoring of the business relationship with these by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination;

10. SIMPLIFIED DUE DILIGENCE

10.1. The simplified due diligence is allowed when the Client representing a low ML/TF risk and in the following cases:
(1) the Client is a company whose securities are admitted trading on a regulated market in one or more EEA Member States, and other companies from third countries whose securities are traded in regulated markets and which are subject to disclosure requirements consistent with EU legislation;

(2) where the Client is a financial institution covered by the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania, or a financial institution registered in another EEA Member State or in the third country which imposes equivalent requirements to those laid down in the laws of the Republic of Lithuania;

(3) the electronic money payment instrument is not reloadable or, where it is reloadable, has a maximum monthly payment transactions limit of EUR 150 and the electronic money payment instrument may be used only in the Republic of Lithuania;

(4) the maximum amount stored on the electronic money payment instrument does not exceed EUR 150;

(5) the electronic money payment instrument is used exclusively to purchase goods or services;

(6) the electronic money stored on the payment instrument cannot be funded with anonymous electronic money;

(7) the electronic money stored on the payment instrument cannot be redeemed in cash.

10.2. **Simplified due diligence cannot apply** if there exist circumstances when the conduction of the enhanced Client identification is required.

10.3. Simplified due diligence also cannot apply, if a separate decision of the European Commission has been adopted on this issue.

10.4. Where it is established that the simplified due diligence can be used, **the Company has to apply measures listed in Annex One.**

10.5. This notwithstanding, the Company must ensure that **supporting documentation is available in the Company**'s **records** and may be made available if required by the relevant authorities.

11. SUSPICIOUS MONETARY OPERATIONS AND TRANSACTIONS

11.1. A transaction which appears unusual is not necessarily suspicious. Therefore, the unusualis, in the first instance, only a basis for further inquiry. This would then require judgment as to whether it constitutes suspicion. Below is the list of criteria of ML and TF which also serve as the examples of the ML/TF activities

11.2. Suspicious transactions are determined by the Employees of the Company when applying the ML/TF prevention measures established under this Procedure and **paying attention to the Monetary operations and Transactions which** according to the documentation and information obtained and the criteria listed below **could be related to ML/TF**. Considering the activity of the Company and the nature of financial services provided by the Company, **Monetary operation or Transaction could be regarded as suspicious, if it meets at least one of the following criteria**:

(1) the monetary operations or transactions of the Client do not correspond to the types of activities specified in the founding documents of the Client or usual cooperation with the Company;

(2) the character of the monetary operations or transactions performed by the Client raises suspicion that it is sought to avoid the inclusion of the monetary operations and transactions in the Register of Monetary Operations Performed by the Client and of Suspicious and Unusual Monetary Operations and Transactions maintained by the Company;

(3) the Client performs monetary operations or concludes transactions where it is difficult or impossible to identify the beneficial owner;

(4) the Client regularly performs monetary operations or concludes transactions with legal persons or other organizations registered in the target territories defined in the Law of the Republic of Lithuania on Corporate Income Tax, where there are no clear economic grounds for such activities;

(5) the Client performs monetary operations or concludes transactions without clear economic grounds;

(6) the Client, the representative of the Client (where the monetary operation or transaction is performed through a representative), beneficial owner or person to whose benefit the monetary operation or transaction is performed is subject to financial sanctions in accordance with the Law of the Republic of Lithuania on the Implementation of Economic and other International Sanctions;

(7) the frequency of small money transfers from different accounts to the account of the Client increases without clear grounds;

(8) the age, job, financial condition of the Client who is a natural person (the income of the Client is too small compared to the scope of his financial activities) objectively fail to correspond to the financial activities carried out by the customer;

(9) the Client's account is transit: funds deposited into the account are soon transferred to another account, while other transactions are almost non-existent;

(10) international payments are made to PEP related natural person, close associate or family member without clear economic grounds**.**

11.3. Suspicious monetary operations or transactions shall be also identified in accordance with the criteria for the identification of suspicious monetary transactions or transactions approved by Resolution No. V-240 of December 5th of 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".

11.4. Proper attention should be given to other circumstances which are not explicitly listed above, but may raise suspicions on ML or TF. Also special attention must be given to the complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible

lawful purpose, and Business relationship or Monetary operations with the End customers from the countries outside the EU and the third countries with the equivalent regime.

11.5. If any suspicious activity listed above or other types of suspicious activity are noticed, **such activity should be immediately reported to the Officer**. If necessary, an investigation of the matter may include gathering additional information internally or from Third parties or other sources as well as suspending the Monetary operation or Transaction and filing a Suspicious Transaction Report with the FIU.

11.6. **EDD measures relating to specific transactions**:

1. requesting a declaration of the source of funds and copies of supporting documents (for example copies of contracts, agreements, inheritance, sale of assets, employment agreements, etc.) for the incoming funds;
2. requesting a declaration of the outgoing payment and copies of supporting documents (for example copies of contracts, agreements, purchase of assets, investment into stocks, etc.);
3. requesting due diligence on the counterparty (payer or payee), such as a description of their business, beneficial owners, managers and directors, banker's reference, etc.

12. ONGOING MONITORING

12.1. After the proper due diligence procedure is undertaken and based on the results of the latter the Client is accepted, the **further monitoring of the Client, its Business relationship (where applicable), Monetary operations and Transactions must apply**. Ongoing monitoring is carried out to ensure that the Clients meet the requirements stipulated in these Procedures and the Company's services are not used for any ML/TF purposes as well as to enable us to establish the possible ML/TF actions and undertake the respective preventative measures.

12.2. Regular monitoring of customer activity and transactions throughout the life of a customer relationship helps BT EXCHANGE (LT) UAB to know their customers.

12.3. BT EXCHANGE (LT) UAB are required to take a risk-based approach to ongoing monitoring, including re-screening for PEPs and sanctions. This is conducted using third party service providers with data screened according to agreed parameters.

12.4. To monitor all the Monetary operations and Transactions undertaken by the Client and be able to assess their consistency with the knowledge, business and risk profile of the Client. During this procedure it must be assessed whether the risk profile, business or financial position of the Client changed throughout the year. Records should be amended to reflect these changes. Previous records should still be kept in file.

12.5. The **Client Due Diligence measures should be also taken every time** where the following circumstances reveal:

(1) when there are doubts about the veracity or adequacy of previously obtained identification data of the Client and/or the Beneficial owner and/or the representative of the Client (where applicable);

(2) in any other case when there are suspicions that the act of ML or TF is, was or will be performed.

12.6. The Company must ensure that **supporting documentation of the ongoing monitoring of the Clients is available in the Company's records** and may be made available if required by the relevant authorities.

13. IN CASE OF SUSPECT

13.1. **Internal Report**. If it is identified by an employee, what is believed to be a suspicious transaction, it must **immediately reported to the AML Officer**. This report should be made in writing and before executing the client's instructions to effect a transaction. An ISAR must be submitted to the MLRO via email with the subject line "ISAR". The MLRO must consider all ISARs.

The email must contain the following information:

- Customer reference number;
- Full name, DOB and Address;
- Description of the reasons of suspicion;

- Transaction in question (if concerns are in respect of a transaction) including:
- Reference number;
- Amount;
- Currency;
- Date (DD/MM/YYYY);
- Description of activity; and
- Merchant information.
- Attach any evidence of the suspicion.

Great care must be taken by staff to ensure that any ISAR is not seen by the customer at any time.

13.2. **Tipping off**. No member of staff or personnel may disclose to the Client concerned or to a third party, the fact that an investigation is being carried out, or that information has been transmitted to the FIU, since such disclosure might prejudice any investigation being carried out. Furthermore, at no stage may any member of staff or personnel, tip off or warn the Client specifically about the Company's reporting obligations or that it has filed a report as this would tantamount to alerting a suspected criminal that the Company has uncovered his illegal activity. Furthermore such tipping off to the Client is likely to prejudice the effectiveness of any investigation or actions in regard to a suspicious Transaction.

13.3. In the event that the Client is inadvertently alerted to ongoing investigations, the Company is to immediately seek guidance from the FIU as to how the Company should act.

13.4. **External report**. When suspicious monetary operation or transaction is detected, a documented investigation must be completed, that operation or transaction must be suspended, and a report made to the FIU within three business hours. There is no minimal threshold or limit for such a report. Once suspicious monetary operation or transaction is reported to the FIU then they are required to respond within ten working days. If the FIU requests further information, then a response to that request must be provided immediately.

13.5. **The Company may be also instructed by the FIU to suspend the particular Monetary operation or Transaction** which the FIU alleges to be a ML/TF mean. In the latter event the Company must suspend such Monetary operation or Transaction **for up to 10 (ten) business days**.

13.6. The FIU must verify the reported Monetary operation or Transaction within 10 (ten) business days as of

the receipt of the respective report or as of the submission of the respective instructions to the Company. **If within 10 (ten) business days** as of the suspension of the Suspicious Monetary operation or Transaction **the Company is not required to perform temporary restriction of ownership rights** according to the procedure established by the Code of Criminal Procedure of the Republic of Lithuania, **the Monetary operation or Transaction has to be resumed**.

13.7. The **FIU may request the Company to provide all necessary information** which is needed for the FIU to carry out the verification of the Suspicious Monetary operation or Transaction. In the latter event the Company must provide the requested information **within 1 (one) business day** after the receipt of the respective request of the FIU.

13.8. **The FIU must be urgently reported** (no suspension is needed) by the Company, if the Company obtains the information that the Client intends or will attempt to perform a Suspicious monetary operation or Transaction.

13.9. The Company shall notify the FIU of the Client's identity data and information on the executed virtual currency exchange transactions (virtual currency purchase or sale in decree currency) or virtual currency transactions (virtual currency asset settlements) the value of a monetary operation or transaction is equal to or greater than EUR 15 000 or currency/virtual currency equivalent, whether the transaction is carried out in the context of one or more related monetary operations. The value of the virtual currency is determined at the time of the monetary operation or transaction.

13.10. The Company has to ensure that any **information requested by the FIU is provided to the FIU within 14 (fourteen) business days**, unless the shorter periods are established in this Procedure or by thelaw.

13.11. The Company, including its Employees acting in good faith, are not responsible to the Client for the non-fulfilment of any contractual obligations and for the damage caused due to the reporting and suspension of the Suspicious Monetary operations and Transactions as well as for the provision of the information upon the request of the FIU.

13.12. **All reports to the FIU must be submitted in the FIU electronic system by filling the respective electronic form of report**. If due to any reasons the submission of the report to the FIU via the FIU electronic system is not available, respective report must be submitted via the e-mail or fax without any delay.

13.13. The FIU may ask for the additional information in writing or via e-mail. In the latter event the requested information must be provided in writing or via e-mail or fax.

13.14. All correspondence with the FIU is to be retained, and that written records of all telephone conversations are made. Copies of all relative documentation are to be kept in the file bearing the name **"Prevention of Money Laundering and Terrorist Funding".**

13.15. **The Officer is to request guidance from the FIU on all relevant matters.**

13. RECORD KEEPING

13.1. The Company must keep the following records:

(1) Client Identification Records:

a. all records of steps taken to obtain identification records, as well as copies of evidence of the identity of the Clients and beneficial owners as the case may be (the documents to be obtained and retained for the Client identification purposes are established in Annex Two to these Procedures);

b. all risk assessment records as well as the Client risk profile;

c. a standard application form must be completed for every new Client as well as for the existing Client where the identification of the Client is needed under these Procedures; the filled application form must be signed off by all the Clients and prospective Clients;

d. all records related to the ongoing monitoring of the Clients.

(2) Record of Transactions:

a. a record containing details of all transactions undertaken in the course of an established Business relationship; this is to include a record of all work performed for or the services provided to the Clients;

b. Transaction records are to be kept in a form which will allow a satisfactory audit trail to be completed where necessary, and which may establish a financial profile of any suspect Client;
c. records on internal and external Suspicious Monetary operations and Transactions reporting.

(3) Other Records:
a. evidence of the training programmes on ML/TF prevention whether in-house or external;
b. evidence of the proper acknowledgment of the Employees with these Procedures and their amendments as may be needed form time to time;
c. other records if required under these Procedures or the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania as well as other legal acts related to the prevention of ML/TF

13.2. **Registers**. The Company keeps the electronic Registers as defined in Section 1 above. **Entries in the Registers must be executed in chronological without any delay, but not later than within 3 (three) business days** as of the respective transaction is executed or the respective circumstances occurred. The Registers are managed and the respective entries in the Registers are made by the Officer, unless other person(s) is(are) appointed by the managing director of the Company.

13.3. The following **data have to be filled** in the Registers:

(1) name, legal form, registration address, code (if available) **for legal person** or its representative (where relevant): name, surname, date of birth, personal number (or another unique combination of characters assigned to the person for identification purposes, if the personal number is not available);

(2) data on the Monetary operation or Transaction: date, description of the assets used (e.g. monetary funds, real estate etc.) and its value, amount, currency;

(3) data on the payee: name, surname, date of birth, personal number (or another unique combination of characters assigned to the person for identification purposes, if the personal number is not available) **for natural person** and company name, legal form, registration address, code (if available) **for legal person;**

(4) data on the Beneficial owner (where applicable) **for the Register of the Suspicious Monetary operations and Transactions as well as the Register of the Clients with whom Transactions or Business relationship has been terminated due to the circumstances related to the ML/TF or the infringement of these Procedures only**: name, surname, date of birth, personal number (or another unique combination of characters assigned to the person for identification purposes, if the personal number is not available);

(5) criterion under which the Monetary operation or Transaction is considered as Suspicious Monetary operation or Transaction in accordance with the order of the Director of the FIU No V-240 of 5 December 2014 **for the Register of the Suspicious Monetary operations and Transactions only;**

(6) reasons for the termination of the Transactions or Business relationship **for the Register of the Clients with whom Transactions or Business relationship has been terminated due to the circumstances related to the ML/TF or the infringement of these Procedures only.**

13.4. The Registers are managed in digital format. The Registers are stored on the servers of the Company and are accessible via the internal network of the Company only. The Registers are managed in the Microsoft Office Excel format. There is possibility to print out the content of the Registers on paper and this possibility remains after the data is copied in other durable medium. The IT system will have back up function which will allow reversing the Registers. Registers' data will be also stored on another server to duplicate all transactions as well as actions within the Company. The IT system allows duplicating information in less than 24 hours.

13.5. **All Client information and documentation have to be kept for the period of 8 (eight) years** as of the end of the Transactions or Business relationship with the Client, **except the correspondence with the Client regarding the business relationship, which has to be kept for the period of 5 (five) years** as of end of the Transaction or Business relationship with the Client.

13.6. The data of the **Registers have to be kept for the period of 8 (eight) years** as of the end of the Transaction or Business relationship with the Client.

13.7. Records may be kept **both in hard copies and in soft copies**, save the Registers which are kept in digital format only.

13.8. **Backups of soft copies** of all Monetary operations and Transactions undertaken are to be taken on a regular basis at least once a month. Certain original documents or certified copies of documents obtained are to be retained in hard copies and these should never be held exclusively in electronic format.

1.	Log of Submitted SARs	To be kept for 8 years after terminating business relationship
2.	Log of virtual currency exchange and transactions equal or greater than EUR 15 000 or currency/virtual currency equivalent	
3.	Log of all customer transactions	
4.	Log of business relationships terminated due to ML/TF reasons	
5.	Copies of ID documents, identification information and KYC information	
6.	Digital currency wallet address together with owner's identity information	
7.	Correspondence with customer	To be kept for 5 years after terminating business relationship
8.	Supporting documents obtained from customer	To be kept for 8 years after completing transaction
9.	Internal investigation records of suspicious transactions	To be kept for 5 years
10.	Other records	To be kept for 8 years

Other records:

· evidence of the training programs on money laundering/terrorism financing prevention whether in-house or external.

· other records if required under the AML law of Lithuania as well as other legal acts related to the prevention of money laundering/terrorism financing.

14. IMPLEMENTATION OF ML/TF PREVENTION MEASURES

14.1. **Implementation of ML/TF Prevention Measures**. The Company's preventative ML/TF measures are adopted taking into account the latest supra-national and national risk assessment documents, including the documents indicated below which shall be reviewed and updated from time to time:

a. the results of the European Commission and national money laundering and terrorist financing risk assessment, unless it is decided during the national money laundering and terrorist financing risk assessment not to comply with certain recommendations of the

European Commission;

b. instructions, as much as they apply to virtual currency exchange operators, approved by the Bank of Lithuania, FCIS;
c. documentation of the European Supervisory Authorities regarding the risks that should be taken into account and the measures that need to be taken in cases when simplified Client identification is permitted;
d. guidelines of the European Supervisory Authorities regarding the risks that should be taken into account and the measures that need to be taken in cases when it is appropriate to apply enhanced Client identification measures.

14.2. The managing director of the Company is responsible for the proper compliance of the Company with the requirements established by the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania as well as other legal acts related to the prevention of ML/TF. Therefore, **the managing director has to arrange the following:**

(1) the preparation and approval of these Procedures as well as proper revision of these Procedures as may be needed from time to time;
(2) the appointment of the Officer and replacement of the Officer as may be needed from time to time as well as arrangement of the respective notification on the latter to the FIU;
(3) ensure the proper acknowledgment of the existing and new Employees with these Procedures as well as the amendments thereto as may be needed from time to time;
(4) ensure the proper trainings of the existing and new Employees on the ML/TF prevention measures prior to their commencement of the duties related to the ML/TF prevention as well as further periodical trainings, including the trainings in case of new ML/TF prevention regulation is issued and/or these Procedures are amended as may be needed from time to time;
(5) ensure the proper implementation of these Procedures in the Company, including but not limited to: due diligence of the Clients; ML/TF risk assessment and management; ongoing monitoring of the Clients; establishment, suspension and reporting of the Suspicious Monetary operations and Transactions; recording and keeping the ML/TF prevention-related information and documentation, including the proper maintenance and keeling of the Registers;
(6) other duties established under the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and other legal acts.

14.3. When performing the above duties the managing director of the Company may appoint other persons to be responsible for the particular duties on the ML/TF prevention in the Company. In such event, the managing director of the Company remains liable under the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and the related legal acts for the proper fulfilment of the above duties.

14.4. The Officer is to be appointed by the managing director of the Company. The managing director of the Company may appoint an alternate the Officer during periods when the Officer is going to beunavailable for a period of time so as to ensure continuity in the Company's obligations related to the ML/TF prevention. **Upon appointment or replacement (whether temporary or permanent) of the Officer the FIU is to be notified on the latter within 7 (seven) calendar days**.

14.5. The Officer is responsible for the oversight of all aspects of the Company's ML/TF prevention activities and is the focal point for all such activity of the Company, including the Client Due Diligence and further ongoing monitoring of the Clients as well as the suspension and reporting to the FIU of the

Suspicious Monetary operations and Transactions and all communication with the FIU.

14.6. If during the Due Diligence stage or later during the ongoing monitoring of the Client the Employee has any doubts regarding the Client or its financial activity, the Employee must apply to the Officer. The Officer has to undertake the needed internal investigation actions and decide if the circumstances reported by the Employee raise high risk of ML/TF. The Officer decides if the Client who raised the doubts can be accepted, which risk category such Client has to be assigned and if the enhanced due diligence and ongoing monitoring have to be undertaken with respect of such Client. All decisions of the Officer as well as reasons for such decisions **should always be documented and retained by the Officer on file.**

14.7. Employees should always file a report to the Officer upon knowledge or suspicion of ML/FT, and it is the Officer who would then consider if a Monetary operation or Transaction has to be suspended and reported to the FIU. If the Officer decides that the Monetary operation or Transaction reported to Officer by the Employee is not a Suspicious Monetary operation or Transaction and there is no need to suspend it and report to the FIU, **the reasons of such a decision should always be documented and retained by the Officer on file**.

14.8. Once an internal report on the Suspicious Monetary operation or Transaction is lodged with the Officer, the latter should then consider the report in the light of all other relevant information in the Company's possession. The Officer is to determine whether the transaction gives rise to knowledge or suspicion that a Client is or could be engaged in ML or TF. The Officer is not expected to investigate the transaction other than internally or to determine whether the funds are the proceeds of criminal activity

14.9. If the Officer is in doubt as to the possibility of ML/TF involvement, he may seek guidance from the FIU. **If the report on the suspicious Monetary operation or Transaction is not filed with the FIU, the Officer should document the reasons for such decision**

15. TRAINING OF EMPLOYEES

15.1. All staff and kept personnel, whose duties include the handling of Clients' business, are to be adequately trained with respect to the procedures and the provisions of the Prevention of Money Laundering Act, the relevant Regulations and the relevant provisions in the Criminal Code of the Republic of Lithuania.

15.2. The level of training provided to individuals is to be appropriate to their role and seniority within the Company. In any case all Employees must have the proper training on ML/TF prevention prior to the commencement of their duties at the Company which involve the ML/TF risk.

15.3. Employees are required to undergo AML/CFT training annually. Employees in high-risk roles or departments will receive additional, role-specific training every six months or whenever they need to be updated on changes to AML/CFT regulations and laws to ensure employees are aware of the latest legal requirements and industry standards

15.4. Training sessions will be delivered through a combination of online modules, in-person workshops, and seminars to cater to different learning preferences. Training materials will include interactive content, case studies, real-world scenarios, and assessments to ensure comprehension and engagement.

15.5. Training will focus on:

(a) identifying various types of money laundering and terrorist financing risks relevant to the organization
(b) practical strategies for mitigating these risks, including proper customer due diligence (CDD), enhanced due diligence (EDD), and ongoing monitoring.
(c) Detailed guidance on how to identify and report suspicious activities, including the use of internal reporting tools and the importance of timely reporting.
(d) Reinforcing the importance of maintaining confidentiality when handling SARs and other sensitive information

15.6. Periodic assessments will be conducted to evaluate employees' understanding of AML/CFT concepts and procedures. Employees must pass these assessments to certify their completion of the training program.

15.7. The training program will be regularly reviewed and updated based on feedback and changes in regulatory requirements.

15.8. All training sessions, including attendance records, assessment results, and certification statuses, will be documented and securely stored. Training records will be maintained to demonstrate compliance with regulatory requirements and to facilitate internal and external audits.

15.9. The managing director of the Company is responsible for the proper performance of the duties related to the training of the Employees. The managing director of the Company may appoint other persons who will undertake all necessary measures for the proper training of the Employees.

Annex One

1. Simplified Due Diligence

1.1. Using the simplified identification procedure, the Company collects only the below indicated information about the Client's identity..

1.2. Following information has to be collected from the personal identification document or the registration document used for the due diligence purposes:

(1) as regards citizens of the Republic of Lithuania:
   a. name(s);
   b. surname(s);
   c. personal number;

(2) as regards foreign citizens;
   a. name(s);
   b. surname(s);
   c. date of birth (if available – personal number or another unique combination of characters assigned to the person for identification purposes);

(3) as regards legal persons (both local and foreign):
   a. corporate name;
   b. legal form, main office (registered office and/or the headquarter in the place of the main interests);
   c. code (registration number etc., if any);
   d. the data of the Beneficial owner;
   e. the activities of a legal person, the purposes and the object of a business relationship, as well as the type of economic activities;
   f. the governance structure and the nature of activity of a legal person.

1.3. When applying the simplified due dilingence, the Company obtaines information indicated in point 1.2 of Annex One and also ensures that the first payment of the Client is performed from the account held in a credit institution, where the credit institution is registered in the European Union Member State or in a third country which has set the requirements equivalent to those laid down in the laws of the Republic of Lithuania and is monitored by competent authorities for compliance with these requirements, except in cases indicated in Section 10.1 (7) of the Procedures.

1.4. In cases indicated in Section 10.1 (7) of the Procedures, the Company can deviate from the measures indicated in Sections 1.1-1.3 of Annex One, however has to perform ongoing monitoring of the Client's Business relationship, including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the Client, the business and risk profile, and the source of funds and to ensure detection of complex or unusually large transactions and unusual patterns of transactions (the Company must analyse the grounds of performance and purpose of such operations or transactions, and execute the results of such analysis in writing).

1.5. Information can be collected either through the face-to-face contact or using electronic means.

1.6. If the thresholds indicated in Section 1.2 are exceeded, the Company must apply the full identification procedure through the face-to-face contact or using non-face-to-face identification measures.

Annex Two

1. Face-to-face contact identification procedure

1.1. Identity of the Clients will be verified through the face-to-face contact pursuant to the below established rules.

1.2. The Client must provide personal identification document (for natural persons) or the registration and/or other corporate documents (for legal persons).

1.3. This Section also applies to those cases where the Client is represented by another person. Usually such representation is documented by the power of attorney. Where the Client is represented by another person, the Employee must identify and verify both the Client and the representative. In addition, the respective **representation document** (usually this will be the power of attorney) **has to be verified** (it is expected that you will check if the person who issued the respective document had such capacity; the validity period of the representation document and the representation powers granted by such document). The representative shall provide personal document (ID or passport) to identify its personality. **Should you have any doubts** regarding the representation document submitted for the identification purposes, you have to apply to the Officer who will assess the representation document submitted and will decide if the submitted document is acceptable for the identification purposes.

1.4. Where the legal person is represented by the managing director of such legal person or by other person who holds the right to represent the legal person under the respective corporate documentation, such situations is considered as the physical presence of the Client and no enhanced due diligence applies. However, the identification of the representative has to be carried out.

1.5. The documents obtained for the identification of the Client have to be sufficient to properly determine and collect the below data and information about the Client and the representative (where applicable).

1.6. Following information has to be collected from the personal identification document or the registration document used for the due diligence purposes:

(1) as regards citizens of the Republic of Lithuania:
   a. name(s);
   b. surname(s);
   c. personal number;
   d. photograph;
   e. signature;
   f. nationality.

(2) as regards foreign citizens;
   a. name(s);
   b. surname(s);
   c. date of birth (if available – personal number or another unique combination of characters assigned to the person for identification purposes);
   d. the number and the expiry date of a permit for permanent residence in a foreign state as well as the place and date of its issue (applies to foreigners permanently residing in a foreign country);
   e. photograph;
   f. signature;
   g. nationality.

(3) as regards legal persons (both local and foreign):
   a. corporate name;
   b. legal form, main office (registered office and/or the headquarter in the place of the main interests);
   c. code (registration number etc., if any);
   d. registration extract and date of its issue;
   e. the data of the Beneficial owner;
   f. the activities of a legal person, the purposes and the object of a business relationship, as well as the type of economic activities;
   g. the governance structure and the nature of activity of a legal person.

2. Identification of the Beneficial owner

2.1. Where the Client is a legal person, the Beneficial owner as defined in Section 1 of the Procedures must be identified (may not apply when the Client is Financial institution). In all cases, the identification of the Beneficial owner means the identification of the **natural person or the group of the natural persons**. For this purpose the Employee has to request the Client to submit the documents which allow identifying the following personal data of the Beneficial owner:

(1) name;
(2) surname;

(3) personal number or another unique combination allowing to identify a person;
(4) nationality.

2.2. Such documents submitted by the Client must be certified in the Client's file or application by the signature and the stamp of the Client, if holding a stamp is mandatory to the Client under the applicable laws. Documents may also be certified on the non-face-to-face basis using a qualified electronic signature.

2.3. In addition, the Employee has to **use the reliable and independent sources** (e.g. Section 8 of the Procedure) for verification of the documents and information regarding the Beneficial owner submitted by the Client. The Employee also has to ask the Client to specify the public sources where the data and documents regarding the Beneficial owner can be verified.

2.4. The following data of the Beneficial owner have to be stored by the Company and available to be submitted to the FIU if required by the latter:

(1) the identity data (name, surname, personal number or another unique combination, if the personal number does not exists);
(2) evidences on verification of the data and documents submitted by the Client in the reliable and independent sources;
(3) data on the management structure of the Client – legal person;
(4) records on the flows of the Client's funds.

2.5. In order to ascertain whether the Client is acting on his own behalf or is controlled, the Employee has to:

(1) verify whether the right to perform a Monetary operation on behalf of the Client has been granted to a person who is in clear business, professional or commercial relations with the Client;
(2) to verify if there are elements that do not correspond to the typical Monetary operations and commercial activity of the Client (e.g. more frequent payments in cash, increasing sums involvedin Monetary operations, Payment for products or services that are not related to the Client's main activity);
(3) to observe if the Client provides requested information in good faith and does not avoid answering the questions.

3. Identification of the PEP

3.1. The PEP is established by verifying the information and documentation provided by the Client. The Employee has to ask the Client indicate and provide relevant information to determine if the Client or the Beneficial owner is a PEP.

3.2. The Employee also has to use additional sources (Section 8 of the Procedures) to establish and/or check the information provided by the Client with regard to the PEPs. Such searches (results thereof) must be documented and stored similarly to the copies of the personal identification documents or other due diligence documents.

4. Identification of the Client registered in the Target territories

4.1. In addition to the above data, where the Client is a legal person or other organisation registered in the Target territory, the Client and its representative (if applicable) must provide in writing the followinginformation:

(1) current place of residence;
(2) postal address;
(3) contact information (valid telephone numbers, email addresses).

5. Information and documentation used for the identification purposes

5.1. The documents submitted for the due diligence purposes must be either:

(1) the original documents; or
(2) the copies certified by the public notary.

5.2. **The Employee has to make and keep the copies of the identification documents** and other documents submitted by the Client for the Client identification purposes when applying face-to-face identification procedure. In case the hard copies are kept, such copies must be:

(1) signed by the Employee, indicating the position, name and surname of the Employee and the date;
(2) marked by the Employee as authentic by making an entry "*True copy*";
(3) certified by the stamp of the Company, if holding a stamp is mandatory to the Company under the applicable laws.

5.3. Additional information obtained from the **Third parties or additional sources** (Section 8 of the Procedures) must be documented and stored similarly to the copies of the personal identification documents or other due

diligence documents as discussed above. Where the checks are made in the data basis or similar sources, the Employee must document the results of such searches/checks, sign and certify such documents in the same manner as the copies of the personal identification documents and store similarly to the copies of the personal identification documents or other due diligence documents.

Annex Three

1. Non-face-to-face identification measures

1.1. Identity of the Clients will be verified through pursuant to the Procedures, including non-face-to-face identification measures established in Section 6.3 of the Procedures, and the below established rules applicable to physical and legal persons.

2. Identification of a physical person

Requirements	Measures
Level 1: **Simplified Due Diligence / Exemptions**	Used when simplified due diligence is applied as described in Annex One. 1. The Client fills in the KYC questionnaire; 2. The Company collects and verifies information as described in Annex One; 3. The Company checks in the consolidated lists of persons, groups and entities subject to the Lithuanian, EU or United Nations financial sanctions: www.urm.lt; http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm; https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list. In case Section 10.1 (1)-(6) of the Procedures is used: 1. The Company additionally requires the Client that the first payment to the electronic money account is done from the Client's bank account.
Level 2: **Unlimited**	The Company uses the following options: 1. Option 1: 1.1. The Client verifies his identity using qualified electronic signature. 2. Option 2: 2.1. The Client's facial image and original identity document is streamed live and compared. The machine readable data is recognized and compared with the entered data by theclient; 2.2. Additional information is collected in the open databases to verify the existence of such person (for instance, name is matched to the date of birth). 3. Option 3: 3.1. The Client's identity document is streamed live, machine readable data is recognized and compared with the data from an advanced electronic signature; 3.2. Additional information is collected in the open databases to verify the existence of such person (for instance, name is matched to the date of birth).

3. Identification of a legal person

Requirements/ Amount of EUR	Measures
One level	After the Company identifies the Client's authorized representative in accordance with identification requirements applicable to physical persons: 1. Client provides the following information in an electronic account opening form: - Name of legal entity (including name in original language); - legal form; - registered and business address; - registration number; - date of registration; - e-mail, business telephone number, web address; - purpose of account and expected transaction types; - estimated incoming payment amount; - indication of origin of funds; - business activity; - beneficial owner declaration. 2. Client uploads the following documents: 2.1. For Clients recorded in the commercial register: - An extract from the Commercial Register issued by the Registrar; or - A written extract (procured by the Company) from a database managed by the registration authority; or - A written extract (procured by the Company) from a reliable, privately managed directory or database. 2.2. For Clients not recorded in the Commercial Register or an equivalent Register: - The by-laws, founding acts or agreements, auditor's certification, official authorization to exercise the activity or equivalent documents; or - A written extract (procured by the Company) from a reliable, privately managed directory or database. Authorities must be identified by means of an appropriate by-law / resolution or other equivalent documents or sources. The extract from the Commercial Register, the certification by the auditor and the directory or database extract must be no more than one year old at the time of identification and must correspond to the current circumstances. 3. Client uploads identification documents of beneficial owner– electronic copy of passport/ ID card. 4. The Company's system verifies through the third party database that the provided information of legal entity and beneficial owner is real, it matches the name and that the person has no criminal history, or is compromised. 5. The information is manually reviewed by the Company's Compliance team and only after this point the Client is allowed to use the account.

Annex Four

The following countries, territories and zones are considered as the **Target territories** under the Procedures:

(1) Andorra
(2) Anguilla
(3) Antigua and Barbuda
(4) Macau
(5) Aruba
(6) Azores
(7) Bahamas
(8) Bahrain
(9) Barbados
(10) Belize
(11) Bermuda
(12) Brunei
(13) Dominica
(14) Jersey
(15) Djibouti
(16) Ecuador
(17) Guernsey, Sark, Alderney
(18) Gibraltar
(19) Grenada
(20) Guatemala
(21) Hong Kong
(22) Jamaica
(23) United Arab Emirates
(24) Cayman Islands
(25) Kenya
(26) Costa Rica
(27) Cook Islands
(28) Kuwait
(29) Lebanon
(30) Liberia
(31) Liechtenstein
(32) Madeira
(33) Maldives
(34) Marshall Islands
(35) Mauritius
(36) Isle of Man
(37) British Virgin Islands
(38) U.S. Virgin Islands
(39) Monaco
(40) Montserrat
(41) New Caledonia
(42) Nauru
(43) Niue
(44) Netherlands Antilles
(45) Panama
(46) Samoa
(47) San Marino
(48) Seychelles
(49) Saint Pierre and Miquelon
(50) Saint Kitts and Nevis
(51) Saint Vincent and the Grenadines
(52) Island of Saint Helen
(53) Tahiti
(54) Turks and Caicos Islands
(55) Tonga
(56) Uruguay
(57) Vanuatu
(58) Venezue