AML Policy

Maxflow Services s.r.o

December 7th 2023

DOCUMENT AUTHOR:	Harry Bedi
DOCUMENT OWNER:	David Kirby
STATUS:	Approved
DATE CREATED:	8/12/2023
VERSION:	1.0
LAST UPDATED:	8/12/2023
SECURITY CLASSIFICATION:	High

VERSION	REVISION DATE	SECTION REVISED	REASON FOR REVISION	DESCRIPTION OF REVISION

Directors Signature 

Date Friday, 08 December 2023

Contents

1 PROCEDURES FOR THE FINANCING OF MONEY LAUNDERING AND TERRORISM AND INTERNATIONAL SANCTIONS

1 PURPOSE

1.1 The purpose of the procedure is to regulate:

- Principles for assessing, managing and mitigating risks related to money laundering and terrorist financing;
- Customer due diligence procedures, including simplified and enhanced customer due diligence Procedures;
- Obligations associated with the collection and disclosure of data on the Actual Beneficiaries of Clients;
- Guidance on how to effectively determine whether a person has a National Background or a Subject of Financial Sanctions or a person who is domiciled or established in a high-risk third country;
- Procedures for collecting, storing and making available data;
- A model for identifying and managing the risks associated with the client and its activities and determining the client's risk profile;
- Methodology and instructions if the Company suspects money laundering and terrorist financing or is an unusual transaction or circumstance, and instructions and procedures for informing the management of compliance with the reporting obligation;
- Refusal to enter into a transaction with the Client and suspension and termination of the Client Relationship;
- Procedures for identifying and managing the risks associated with new and existing technologies and services and products, including new or non-traditional sales channels and new or evolving technologies.
- Obligations related to the collection and publication of data of user account holders; Rights and obligations of the contact person;
- The Company's Risk Assessment and Risk Appetite;
- Responsibility for checking the compliance of the Procedure with the requirements and the proper compliance of the Procedure with the Managers and Employees.

2 RESPONSIBILITY

2.1 The Contact Person of the Financial Intelligence Unit is responsible for checking the compliance of the procedure with the requirements and its proper compliance.

2.2 The procedure is mandatory for all Managers and Employees.

3 GENERAL PROVISIONS

3.1 The procedure has been established for the fulfilment of the requirements arising from the AML/CTF Law and includes the rules of procedure for the proper fulfilment of the obligations to prevent the financing of money laundering and terrorism and the implementation of the Financial Sanctions, as well as the internal control rules.

3.2 The Company and its Managers and Employees are obliged to pay close attention to the activities and circumstances of a person participating in a transaction or official activity, a person using professional services or the Client, which indicate money laundering or Terrorist Financing or are likely to be related to and unusual transactions that do not have a reasonable economic purpose.

3.3 The Company and its Managers and Employees are obliged to pay special attention to the business relationship or transaction in their activities, if the Client or the person or professional service participating in the transaction

The user or the payee's payment service provider is located in a third country or territory where adequate anti-money laundering and anti-terrorist financing measures have not been adopted or where that country or territory does not cooperate internationally in the prevention of money laundering and terrorist financing or has a low tax rate territory. Low-tax territories are all territories, except Czech Republic, which are not mentioned in Regulation No. 55 of the Minister of Finance of 18 December 2014. A list of countries that have not adopted adequate anti-money laundering and anti-terrorist financing measures is available at http://www.fatf-gafi.org/countries/#high-risk.

3.4 Particular attention must be paid to the activities of the Client participating in the transaction and to circumstances that indicate money laundering or terrorist financing or are likely to be involved in money laundering and terrorist financing, including complex, high-value and unusual transactions that do not have a reasonable economic purpose.

3.5 In order to fulfil the obligation set forth in the Procedure, the Company applies the following due diligence measures:

3.5.1 Identification of the Client or his / her representative and verification of the submitted information on the basis of information obtained from a reliable and independent source, including by means of e-identification and e-transaction trust services;

3.5.2 Identification and verification of the identity and right of representation of the Client or his / her representative;

3.5.3 Identification of the Actual Beneficiary and the introduction of measures to verify his / her identity to the extent that enables the Company to ascertain who is the Actual Beneficiary of the Client and understands the ownership and control structure of the Client;

3.5.4 Understanding the business relationship or the Instructions and, where appropriate, collecting additional information thereon, specifying, inter alia, the Client's domicile, business or area of residence, professional or field of activity, major counterparties, payables and, in the case of a legal entity, experience;

3.5.5 Obtaining information on whether the Client or his / her representative is a Person with a State Background;

3.6.6 Continuous monitoring of the Customer Relationship, including monitoring of transactions performed during the Customer Relationship, regular verification of the data used to establish identity, updating of relevant documents, data and information and, if necessary, identification of the source and origin of funds used in the transaction.

3.6 The Company has applied due diligence measures if the Company and the Employee or Manager who has implemented the due diligence have an internal belief that they have complied with the due diligence obligation to clarify the possible involvement of the transaction, operation or funds in Money Laundering or Terrorist Financing. The principle of reasonableness shall be taken into account in assessing the emergence of such an internal conviction.

3.8 The Company offers the Service only to Customers who, in the case of a natural Customer, confirm by filling in the Identification Form that they are not a State Background, and the legal representative confirms that they are not, the Customer is not, and the Ultimate Beneficiary is not a State.

3.9 The Company does not offer its services to an individual Customer who is not a Real Beneficiary. If the Company suspects that the individual Customer is not the Actual Beneficiary, regardless of the Customer's confirmation, the Company will request additional information from the Customer. If the Customer refuses to provide the data, the Company shall suspend the performance of the Customer Agreement and, if necessary, block the User Account and

The contact person will inform the Financial Intelligence Unit. Doubt as to the existence of a Real Beneficiary may arise, in particular, if the Company, in applying due diligence measures, suspects that a natural person has been inclined to enter into a business relationship or enter into a transaction.

3.10 In order to use the Company's service in the Customer Environment, a User Account shall be created for the Customer in the Customer Environment, through which the Customer may submit Instructions to the Company. After creating a User Account, but before submitting the first Instruction, the Company will establish the identity of the Customer:

- In accordance with the requirements set out in the Regulation of the Minister of Finance of the Czech Republic “Technical Requirements and Procedure for Identification and Verification of Data by Information Technology Means”, developing an IT solution or transferring the respective activity to a Third Party in accordance with Part 4 of the Internal Rules. Procedures for the transfer of activities';
- Staying in the same place as the Client.

3.11 If necessary, the Company shall identify the source and origin of the funds used by the Clients in the transaction.

3.12 The source and / or origin of the funds used in a transaction must be identified, in particular if:

- There is a suspicion that these may be transactions related to Money Laundering or Terrorist Financing;
- There is a suspicion that the Customer or the party to the transaction is a Person with a State Background;
- A significant increase in the funds used in the transaction, which differs significantly from past payment behaviour;
- the transactions do not correspond to the information previously known about the customer.

3.13 At the request of the Company, the Client participating in the transaction performed in economic and professional activities shall submit the documents necessary for the application of due diligence measures and provide relevant information. At the request of the company, the Client or his / her representative shall confirm the accuracy of the information and documents submitted for the application of due diligence measures with his / her signature in the transaction performed in economic and professional activities.

3.14 The due diligence measures specified in Section 3.6 apply to:

- Creating a customer relationship;
- In case of doubt as to the adequacy or veracity of documents or data previously collected in the course of verifying the information gathered through the application of due diligence or updating relevant data;
- In case of suspicion of money laundering or Terrorist Financing.

4 APPLICATION OF MAINTENANCE MEASURES IN A SIMPLIFIED PROCEDURE

4.1 The Company may apply due diligence measures in a simplified manner if the Risk Assessment prepared by the Company determines that its economic or professional activity, field or circumstances present a lower-than-usual risk of Money Laundering or Terrorist Financing.

4.2 Before applying the simplified due diligence measures to the Client, the Company determines that the business relationship, transaction or operation is of lower risk, using the information approved by the Management Board.

“Customer Risk Level Identification Model” and information known to the Company about the Customer and the Instructions submitted by the Customer.

4.3 The application of the due diligence procedure is permitted to the extent that the Company ensures adequate monitoring of transactions, operations and business relationships to enable the detection and reporting of unusual or suspicious transactions in accordance with the Procedure.

4.4 When implementing the due diligence measures in a simplified manner, the Management Board may determine the extent of the fulfilment of the obligation and the need to verify the source of the information used for this purpose and the data from a reliable and independent source.

4.5 The Client's Business Relationship Monitoring may be applied in a simplified manner if a circumstance characterizing a lower risk has been identified in the Client's case and if at least the following conditions are met:

4.5.1 A Customer Agreement has been entered into with the Customer in written, electronic or in a form that can be reproduced in writing;

4.5.2 The Company receives payments within the framework of the Business Relationship only through an account located in a credit institution registered in Czech Republic, or the United Kingdom or in a branch of a foreign credit institution established or domiciled in a Contracting State of the European Economic Area or in a country applying Directive (EU) 2015 / 849 requirements equivalent to the requirements;

4.5.3 The total value of incoming or outgoing payments for transactions made in a business relationship does not exceed 15,000 euros per year.

4.6 When assessing a circumstance indicating a lower risk, at least the situation where the Client is:

4.6.1 a company listed on a regulated market which is subject to disclosure obligations which impose requirements to ensure sufficient transparency for the Beneficial Owner;

4.6.2 a legal person in public law established in Czech Republic;

4.6.3 a government agency of Czech Republic or a Contracting State of the European Economic Area or another institution performing public functions;

4.6.4 European Union agency;

4.6.5 a credit institution or financial institution acting in its own name, a credit institution or financial institution located in a Contracting State of the European Economic Area or in a third country subject to requirements equivalent to those of Directive (EU) 2015/849 of the European Parliament and of the Council in its country of supervision;

4.6.6 The Client is domiciled in the following country or geographical area:

4.6.6.1 in a Contracting State of the European Economic Area;

4.6.6.2 in a third country with effective systems to prevent money laundering and terrorist financing;

4.6.6.3 in a third country where, according to reliable sources, the level of corruption and other criminal activity is low;

4.6.6.4 in a third country where, according to reliable sources, such as peer reviews, reports or published follow-up, anti-money laundering and anti-terrorist financing requirements are in place in line with the revised recommendations of the Financial Action Task Force and are effectively implemented.

5 APPLICATION OF DUE DILIGENCE MEASURES

5.1 The Company will apply enhanced diligence measures to adequately manage and mitigate the higher than usual risk of money laundering and terrorist financing associated with the Service, or if:

5.1.1 Upon establishing the identity of the Customer or verifying the submitted information, the Company has doubts about the veracity of the submitted data or the authenticity of the documents or identification of the actual beneficiary;

5.1.2 a person participating in a transaction or official act performed in an economic or professional activity, a person using professional services or a client is a Person with a State Background;

5.1.3 the person participating in the transaction or official activity performed in the economic or professional activity, the person using the professional service, or the Client originates or is domiciled, or the payee's payment service provider is located in the Sanction Country (Annex 2), Low Tax Territory (Annex 2), Other high-risk territory (Appendix 3);

5.1.4 The customer or person using the transaction or the person using the professional services originates in or resides in a country or territory where the payee's payment service provider is located in a country or territory where, according to reliable sources such as peer reviews, reports or published follow-up reports, put in place effective anti-money laundering and anti-terrorist financing systems in line with the recommendations of the Financial Action Task Force.

5.1.5 The Company will apply enhanced diligence measures even if the resulting Risk Assessment identifies a higher than usual risk of Money Laundering or Terrorist Financing for this Service, area or circumstance, if the European Supervisory Authorities have issued appropriate guidelines on risk factors, and the following major Circumstances characterizing the risk:

5.1.5.1 Related to the Client's person:

- The business relationship operates in unusual circumstances, including complex and unusually large transactions and unusual transaction patterns that do not have a reasonable, clear economic or legitimate purpose or are not specific to the specific business;
- The Client is a resident of the higher risk geographical area specified in clause 5.1.3 of these Procedure;
- The client is a legal entity or other association of persons without the status of a legal entity that is engaged in personal asset management;
- The customer is a company handling large amounts of cash;
- The client or related company has shareholders or bearer shares;
- The ownership structure of the client company seems unusual or too complex in view of the company's activities;
- Negative information about the customer is known (https://namescan.io/FreeAdverseMediaCheck.aspx#gsc.tab=0);
- The client is listed in the International Sanctions List (https://namescan.io/FreeSanctionsCheck.aspx, https://www.sanctionsmap.eu/#/main).

5.1.5.2 Related to a service, transaction or transmission channel where:

- Private banking;
- Offering or brokering a product or transaction that may promote anonymity;
- Payments received from unknown or unrelated third parties;
- A business relationship or transaction that is established or initiated in a manner that does not involve the customer, its agent or a party to the transaction and is not subject to IT verification as a safeguard;
- New products and new business practices, including the use of a new transmission mechanism or new or evolving technology for both new and existing products.

5.1.5.3 As a circumstance that increases geographical risk in a situation where the Client, a person participating in the transaction or the transaction itself is related to the state or jurisdiction:

- Where, according to reliable sources, such as peer reviews, detailed evaluation reports or published ex-post reports, effective anti-money laundering and anti-terrorist financing systems are not in place;
- Where, according to reliable sources, the level of corruption or other criminal activity is significant;
- Subject to sanctions, embargoes or similar measures, such as those imposed by the European Union or the United Nations;
- Which finances or supports terrorism or in whose territory terrorist organizations designated by the European Union or the United Nations operate.

6 ADDITIONAL MAINTENANCE MEASURES

6.1 In determining the higher-than-usual risk of Money Laundering and Terrorist Financing, the Company will apply one or more of the following due diligence measures in its analysis and mitigation of risks:

- Verifying additional information submitted in connection with the identification on the basis of additional documents, data or information from a reliable and independent source;
- Gathering additional information about the purpose and nature of the business relationship, transaction or operation and verifying the information provided on the basis of supporting documents, data or information from a reliable and independent source;
- Collecting additional information and documents about the actual execution of transactions in the business relationship to rule out the appearance of transactions;
- Collecting additional information and documents to identify the source and origin of the funds used in the transaction to prevent the transactions from appearing;
- Requiring the Customer to make the first payment related to the transaction through an account opened in the name of the person or customer participating in the transaction with a credit institution registered or established in a Contracting State of the European Economic Area or in a country equivalent to Directive (EU) 2015/849 requirements;
- By applying due diligence measures to the person or his representative while in the same place.

6.2 In identifying the risks of heightened Money Laundering and Terrorist Financing and applying enhanced due diligence measures, the Company shall monitor the Business Relationship more frequently than usual, including no later than six months after the commencement of the Business Relationship to assess the Client's risk profile.

7 ENHANCED DUE DILIGENCE MEASURES APPLICABLE TO TRANSACTIONS WITH A HIGH-RISK NATURAL OR LEGAL PERSON IN A THIRD COUNTRY

7.1 If the Company comes into contact with a country listed in Appendix 1, Appendix 2 and Appendix 3 through a person participating in the provision of the Service or an official activity, a person using the professional service or a client, Employees must additionally apply one or more of the following due diligence measures:

- Obtain additional information about the Client and his / her actual beneficiary;
- Obtain additional information about the planned content of the business relationship;
- Obtain information on the funds and the origin of the wealth of the Client and his / her Actual Beneficiary;
- Obtain information on the reasons for the transactions planned or performed by the Client;
- Approve the establishment or continuation of a business relationship with the Management Board;
- In co-operation with the Contact Person, a decision will be made to improve the monitoring of the business relationship by increasing the number and frequency of control measures applied and selecting transaction indicators to be further checked;
- Requiring the Customer to make a payment to an account in the name of the Customer from a credit institution of a Contracting State of the European Economic Area or a third country applying requirements equivalent to the requirements of Directive (EU) 2015/849 of the European Parliament and of the Council.

7.2 In case of additional information and documents received, the Employees must make a decision in accordance with the Client's profile and risk assessment and in the event of unusual or suspicious signs, immediately notify the Contact Person of the Company's internal Money Laundering or Terrorism suspicion of financing.

8 IDENTIFICATION IN ESTABLISHING CUSTOMER RELATIONSHIPS AND TRANSACTIONS

8.1 The Investigator is obliged to apply the following rules of the Procedure for Identification each time before establishing a Client Relationship, when applying regular due diligence measures, in case of suspicion of Money Laundering and Terrorist Financing and in case of application of International Sanctions.

8.2 The Company and its Employees are prohibited from performing a transaction or concluding a Customer Agreement with a Customer who refuses to provide information, documents or relevant information requested by the Company. Also, with Clients in respect of whom the Employee has a suspicion of an ambush or in the case of data, documents or relevant information provided by the Employee, the Employee has a suspicion that it may be Money Laundering or Terrorist Financing.

8.3 In case of doubt, the Employees must immediately inform the Contact Person and record as much information as possible, which will help to identify and prove the subsequent circumstances.

9 IDENTIFICATION OF A NATURAL PERSON IN THE SAME PLACE

9.1 The Employee shall identify the Customer and, where applicable, his or her representative and shall retain the following information about the person and, where applicable, his or her representative:

9.1.1 First name and surname;

9.1.2 Personal identification code, in the absence thereof, date and place of birth and place of residence or seat;

9.1.3 information on the identification and control of the right of representation and its scope, and if the right of representation does not arise from law, the name of the document on which the right of representation is based, the date of issue and the name of the issuer.

9.2 The following valid documents specified in subsection 2 (2) of the Identity Documents Act may be used as the basis for establishing the identity of a natural person:

- Identity card;
- Digital identity card;
- Residence permit card;
- Passport of a Czech Republic citizen;
- Diplomatic passport;
- Seaman's service book;
- An alien's passport
- Temporary travel document;
- A refugee's travel document;
- Certificate of competency
- Permission to return;
- Driving license issued in the Republic of Czech Republic; or
- Travel document issued abroad (foreign passport)

9.3 The employee shall make a copy of the personal data and photo page of the identity document and, in the case of third-country nationals staying in the Czech Republic who are required to have an entry visa, a copy of a valid entry visa and a border crossing stamp. The signature and date of the person making the copy shall be attached to the copy.

9.4 If the original document specified in clause 9.1.4 of this Procedure cannot be seen, the Employee may use the notarised or notarised or officially certified document referred to in subsection (3) or other information from a reliable and independent source, including e-identification and e-transaction trust services, to verify identity. using at least two different sources to verify the data.

9.5 The employee shall verify the accuracy of the information specified in clauses 9.1.1 and 9.1.2 of the Procedure and the validity of the documents specified in 9.1.4 by searching for the documents issued in the Czech Republic. Document validity checks / or using information from another reliable and independent source accepted by the Management Board.

9.6 If an identifiable person has a valid document specified in clause 9.1.4 of the Procedure or a document equivalent to this document and his or her identity is established and verified on the basis of the specified document or by means of e-identification and e-transaction trust services and the validity of the document is evident or identifiable -identification and e-transaction trust services, no additional data on the document need be retained.

10 IDENTIFICATION OF NATURAL PERSONS AND VERIFICATION OF DATA THROUGH INFORMATION TECHNOLOGY

10.1 Identification of the Customer and, where applicable, his / her representative and verification of data by means of information technology is mandatory for the Company if:

10.1.1 A business relationship is established with an e-resident or a person who is from or resides in a country outside the European Economic Area and where the due diligence measures are not applied while in the same place as the person or his / her representative;

10.1.2 A business relationship is established with a person who is from or resides in a Contracting State of the European Economic Area and whose total outgoing payments related to the Customer Agreement in one calendar month exceed 15,000 euros in the case of a retail customer and 25,000 euros in the case of a legal customer. due diligence measures shall not be applied while the person or his representative is in the same place.

10.2 If the person is a foreign citizen, a valid travel document (e.g. passport), in addition to the digital identity document issued in the Czech Republic or another high-reliability e-identification system entered in the e-identification and e-identification system of Regulation (EU) No 910/2014 of the European Parliament and of the Council, repealing the list published in the Official Journal of the European Union pursuant to Article 9 of Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73–114).

10.3 The Company shall develop an IT solution or enter into an agreement with a Third Party for the use of the identification and data verification service for the purpose of identification and data verification by means of information technology means, which is in accordance with the technical requirements and procedures established by the Regulation of the Minister of Finance of the Czech Republic.

11 IDENTIFICATION OF LEGAL ENTITIES

11.1 The company shall identify the identity of a legal person registered in the Czech Republic and a branch of a foreign company registered in Lithuania and a foreign legal person and shall retain the following information concerning it:

11.1.1 Business name or name of the legal person;

11.1.2 Registry code or registration number and time;

11.1.3 the name of the director or the names of the members of the management board or other bodies replacing him or her and their powers to represent the legal person;

11.1.4 Data on the means of communication of a legal person.

11.2 The Company shall verify the accuracy of the information specified in clauses 11.1.1 and 11.1.2 of this Procedure, using information from a reliable and independent source.

11.3 The Company shall establish the identity of a legal person on the basis of the following documents:

11.3.1 the registry card of the relevant register;

11.3.2 Registration certificate of the relevant registry or

11.3.3 A document equivalent to the document specified in clauses 11.2.1 or 11.2.2.

11.4 If the Company has access to the data of the commercial register of the Czech Republic or relevant registers of a foreign country via a computer network, the Client need not be required to submit the documents specified in clause 11.3 and its sub-clauses.

11.5 If it is not possible to see the original document specified in clause 11.3 of this Procedure, notarised or notarised or officially certified documents or other information from a reliable and independent source, including e-identification and e-transaction trust services, may be used to verify the identity of the Legal Entity. at least two different sources for verifying the data.

11.6 A representative of a foreign legal entity must submit to the Company a notarised or equivalent document certifying its authority, which has been legalized or certified by a certificate substituting for legalization (apostille), unless otherwise provided by an international agreement.

12 ACTUAL BENEFICIARY AND ITS IDENTIFICATION

12.1 Upon identification of a legal entity, the Company must register the Actual Beneficiary of the legal entity. It is generally presumed that a legal person is represented by a legal representative, or a person authorized to do so. Proxies and other documents issued abroad must be legalized or apostilled. When dealing with a document containing the right of representation, it must also be ascertained whether the persons who issued it had the respective competence. A person representing a legal person is required to know the economic and professional activities of that person, the purposes of the transactions, the business partners, the source and origin of the funds used in the transactions, the circle of owners, etc.

12.2 The Company shall record and maintain information on all actions taken to identify the Beneficial Owner.

12.3 If the Client is a company whose securities are admitted to trading on a regulated securities market, it is not necessary to identify the Actual Beneficiaries of such company.

12.4 Information received from the representative of a legal entity shall be used to identify the beneficial owner.

12.5 The Employee shall analyse the documents submitted by the representative of the legal entity and, if necessary, request additional documents and data in order to identify the Actual Beneficiary (i.e.) of the legal entity.

12.6 If the Employee has doubts about the accuracy or completeness of the respective information, he / she shall check the submitted information from publicly available sources and, if necessary, request additional information from the person. If necessary, the Contact Person will be consulted

12.7 If the identity documents of the legal entity or other submitted documents do not directly show who the Actual Beneficiary of the legal entity is, the respective data shall be registered on the basis of the testimony of the representative of the legal entity or his / her own written document after consulting the Contact Person. In order to verify the accuracy of the information established on the basis of testimony or a handwritten written document, the Company must take reasonable measures (requesting the relevant registers), requiring the submission of the annual report of the legal person or other relevant document.

12.8 In determining the beneficial owner, special attention must be paid to companies established in low-tax areas (Annex 2), the legal capacity of which is not always unambiguous.

12.9 If another legal entity has control over a legal entity in accordance with the definition of a Real Beneficiary, the Employee must assess the risk of the person or client and collect data on other legal entities related to the other person to identify the Real Beneficiary.

12.10 Upon identification of the Actual Beneficiary of a natural person, in case of doubt, the Company must also identify the Actual Beneficiary of the natural person, i.e., the person controlling the activities of the person, in order to avoid the risks related to the use of undercover agents.

12.11 Doubts as to the existence of a Real Beneficiary may arise in particular if, when implementing due diligence measures, the Employee has a feeling that a natural person has been inclined to establish a business relationship or enter into a transaction. In this case, the person exercising control over the natural person must be considered the Real Beneficiary of the natural person.

13 POLITICALLY EXPOSED PERSONS (PEPs), IDENTIFICATION AND REFUSAL OF TRANSACTIONS

13.1 The Company does not offer the Service to PEPs, Customers whose owner or Actual Beneficiary is a PEP or if a PEP participates in transactions.

13.2 This principle applies to both local and foreign politically exposed persons.

13.3 If a PEP has no longer performed the important public duties assigned to him or her within 12 months, the Employee must make a corresponding written decision on the absence of the status of a PEP from the Management Board or the Contact Person.

13.4 When establishing a Customer Relationship, the Company shall determine the status of Persons with a State Background in respect of all Customers or if the Company has reason to believe that such a connection exists when offering the Service and applying due diligence measures.

13.5 Upon identification of Persons with a State Background, upon receipt and execution of the Instructions, the Company shall refrain from complying with the Instructions and return the funds of the Instructions to the Client.

13.6 In order to identify Persons with a National Background, the Company will develop an IT solution, enter into an agreement to use the service provided by a Third Party or make a manual inquiry from a publicly accessible independent source (https://namescan.io/FreePEPCheck.aspx).

14 BUSINESS RELATIONSHIP MONITORING

14.1 Monitoring of the business relationship is one of the most important methods for identifying the Company's suspected money laundering or Terrorism in the provision of the Service.

14.2 In the course of monitoring the business relationship, the transactions performed by the Employee, or the information system used in the Business Relationship on the basis of the Client's Transactions and their volumes shall be performed to ensure that the transactions are in accordance with the Company's knowledge of the Client, its activities and risk profile.

14.3 The Company shall monitor the Business Relationship during the implementation of due diligence measures, using a risk-based approach in accordance with the risk classes assigned to the Clients when establishing the Client Relationship and on a random basis upon receipt of the Transactions.

14.4 In the course of monitoring the business relationship, the Employee is obliged to analyse the origin of the funds used in the Transactions and their compliance with the Client's economic capacity.

14.5 In the course of monitoring the business relationship, the Employee is obliged to check the validity of the documents used to identify the Customer and make inquiries to Adverse Media (https://namescan.io/FreeAdverseMediaCheck.aspx#gsc.tab=0), PEP (https://namescan.io/FreePEPCheck.aspx) and Sanctions (https://namescan.io/FreeSanctionsCheck.aspx) manually or through an IT solution developed by the Company.

14.6 If necessary, the Employee is obliged to ask the Client:

- Additional documents (annual reports, account statements) showing the original sources of funds;
- Additional information about the Client and his / her Actual Beneficiary;
- Additional information on the funds and wealth of the Actual Beneficiary

14.7 The Employee shall pay greater attention to circumstances that indicate criminal activity, Money Laundering or Terrorist Financing or are likely to be related to Money Laundering or Terrorist Financing, including complex, high value and unusual transactions and transaction patterns that do not have a reasonable or visible economic or legitimate purpose; which is not specific to a particular business. In fulfilling this obligation, the nature, cause and background of these transactions must be clarified, as well as other information to understand the content of the transactions, and greater attention must be paid to these transactions. These include:

- The customer buys virtual currencies in one transaction worth more than 32,000 euros.
- A single large purchase or sale of virtual currencies using a service that makes it difficult to identify one or more persons involved in a virtual currency transaction, such as a tumbler or mixer.
- A politically exposed person (PEP) has bought or sold virtual currencies worth more than 10,000 euros.
- A virtual currency transaction uses the services of intermediaries that guarantee / complicate the impossibility or difficulty of identifying a person (for example, service providers who allow personal data not to be passed on to law enforcement authorities).
- Assets worth more than 32,000 euros are purchased for the virtual currency.
- The customer is paid for the virtual currency in the account of a third party (except for the payment service provider or the service provider related to the exchange and intermediation of virtual currencies, whose business is the intermediation of such payments).

- The customer purchases virtual currencies with more than 32,000 euros in several related transactions.
- The client sells virtual currencies worth more than 32,000 euros in several consecutive transactions, the origin of the virtual currencies is unknown.
- Regular buying and selling of virtual currencies through the services of intermediaries guaranteeing / making it impossible or difficult to identify a person (for example, service providers who allow personal data not to be passed on to law enforcement).
- Regular buying and selling of virtual currencies using a service that makes it difficult to identify a person making one or more transactions in virtual currencies, such as a tumbler or mixer.
- A person collects or transfers funds or virtual currency to a person affiliated with a terrorist organization or located in known areas of terrorism.

14.8 In its economic, professional or professional activities, the Company must pay special attention to the Business Relationship or Instructions if the parties to the transaction are exposed to high risk from a third country or territory specified in Annex 1, Annex 2 and Annex 3 to the Internal Rules the payee or the payee's payment service provider is located in that country or territory.

14.9 In case of doubts arising during the monitoring of the business relationship, which cannot be dispelled by the explanations received from the Client, the Employee is obliged to immediately notify the Contact Person of the doubts.

15 DATA RECORDING, VERIFICATION AND STORAGE

15.1 The Company shall record the date or period of making and executing the Order and a description of the content of the transaction. In addition, the Company registers:

15.1.1 Information on the circumstances of the Company's refusal to establish a business relationship or occasionally to enter into a transaction;

15.1.2 the circumstances of the establishment of a business relationship or the waiver of a transaction, including the conclusion of a transaction, on the initiative of a person participating in a transaction or official act, if the waiver is related to the application of due diligence measures by the Company;

15.1.3 Information if the due diligence measures specified in subsection 20 (1) of the AML/CTF Law and clauses 4,5,6 and 7 of this Procedure cannot be applied by means of information technology means;

15.1.4 Information on the circumstances of termination of the Business Relationship in connection with the impossibility of applying due diligence measures;

15.1.5 in the case of suspicion of money laundering and terrorist financing, the information on which the notification obligation is based;

15.1.6 The Company shall keep the originals or copies of the documents specified in clauses 9.10 and 11 of the Procedure and the documents on the basis of which the Business Relationship is established for five years after the termination of the Business Relationship.

15.1.7 The Company shall keep for five years all correspondence and documents collected in the course of the monitoring of the Business Relationship related to the fulfilment of the obligations arising from the AML/CTF Law, as well as data on suspicious or unusual transactions or circumstances that were not reported to the FIU.

15.1.8 The company must keep the documents prepared on the transactions on any medium and the documents and data on which the obligation to report money laundering or terrorist financing is based for at least five years after the transaction has been performed or the notification obligation has been fulfilled.

15.1.9 The Company shall keep documents and records in a manner that allows for an exhaustive and immediate response to inquiries from the FIU or other supervisory authorities, investigative bodies or courts as required by law, including whether the Company has or has had a business relationship with the person named in the inquiry. is or was the nature of that relationship.

15.1.10 If the Company makes a request to the database belonging to the State Information System for identification, the obligation to store the request data shall be deemed fulfilled if the information on making an electronic request to the specified register is reproducible within five years after the termination of the business relationship or transaction.

15.1.11 The Company shall retain the data of the digital identification document, information on making an electronic search of the identity document database and the audio and video recording of the identification and verification procedure for five years after the termination of the business relationship when implementing the means of identification and verification using information technology.

15.1.12 The Company applies all personal data protection rules when applying the requirements arising from the AML/CTF Law.

15.1.13 The Company is allowed to process personal data collected during the implementation of the AML/CTF Law only for the purpose of preventing Money Laundering and Terrorist Financing, and such data may not be further processed in a way that does not meet this purpose, for example for marketing purposes.

16 MEMBER OF THE MANAGEMENT BOARD AND CONTACT PERSON

16.1 If the Company has more than one member of the Management Board, the Company shall appoint a member of the Management Board who is responsible for the implementation of AML/CTF Law and the legislation and guidelines established on the basis thereof.

16.2 The Management Board shall appoint a person who is the Contact Person of the Financial Intelligence Unit, who reports directly to the Management Board and who has the competence, resources and access to relevant information in all structural units of the Company necessary for the performance of the tasks provided by AML/CTF Law. If a Contact Person has not been appointed, the duties of the Contact Person shall be performed by a member of the Management Board, or a member of the Management Board appointed in accordance with clause 16.1.

16.3 The duties of a contact person may be performed by an Employee or a structural unit. If the functions of the Contact Person are performed by a structural unit, the head of that structural unit shall be responsible for the performance of the functions of the Contact Person. The Financial Intelligence Unit and the competent supervisory authority shall be notified of the appointment of the contact person.

16.4 Only a person who has the education, professional suitability, necessary abilities, personal qualities and experience and impeccable reputation necessary for the performance of the duties of the Contact Person may be appointed as a Contact Person.

16.5 The appointment of a contact person shall be approved by the Money Laundering Information Bureau.

16.6 The Financial Intelligence Unit has the right to receive information from the Contact Person or the Contact Person Candidate, the Company and state databases in order to check the suitability of the Contact Person or the Contact Person Candidate. If, as a result of an inspection performed by the Financial Intelligence Unit, it is revealed that the person's reliability is in doubt due to his or her previous actions or omissions, the person's reputation is not impeccable, and the Company may terminate the Contact Person's employment contract. If the functions of the Contact Person are performed by a structural unit, the provisions of this subsection shall apply to each employee of that structural unit.

16.7 The duties of the contact person are, inter alia:

16.7.1 Arranging and analysing the collection of information referring to unusual or suspected Money Laundering transactions or circumstances or Terrorist Financing within a maximum of two business days of becoming aware of the suspicion (either through a notification sent by the Employee or through independent monitoring);

16.7.2 Transmission of information to the Financial Intelligence Unit in case of suspicion of Money Laundering or Terrorist Financing;

16.7.3 Submission of periodic written reviews to the Management Board on compliance with the requirements arising from AML/CTF Law;

16.7.4 Fulfilment of other obligations related to the fulfilment of the requirements of the AML/CTF Law.

16.8 The contact person has the right to:

16.8.1 To make proposals to the Management Board for amending and supplementing the Internal Rules containing the requirements for the prevention of money laundering and terrorist financing and for organizing trainings related to the prevention of money laundering and terrorist financing;

16.8.2 Require the structural unit of the Company to eliminate the deficiencies identified in the compliance with the requirements for the prevention of money laundering and terrorist financing within a reasonable time;

16.8.3 Send the data and information necessary for the performance of the duties of the Contact Person;

16.8.4 Make proposals for the organization of the process of submitting suspicious and unusual notifications;

16.9 Receive training in the field.

16.10 The contact person may only pass on information or data that has become known to him or her in connection with a suspicion of money laundering or terrorist financing:

- Financial Intelligence Unit;
- The pre-trial investigation authority in connection with criminal proceedings; To a court on the basis of a court order or decision.

16.11 Each Employee must notify the Contact Person of all cases of refusal to establish a business relationship on the basis of the AML/CTF Law, suspected or unusual transactions of Money Laundering or Terrorist Financing, and cases of extraordinary cancellation of Customer Relationships.

16.12 If an Employee identifies activities or circumstances in the course of his or her economic or professional activities or official activities, the characteristics of which indicate Money Laundering or Terrorist Financing or in which he / she knows that it is Money Laundering or Terrorist Financing, he / she shall immediately notify the Contact Person. In urgent cases by telephone and later in writing.

16.13 In identifying suspicious transactions, the Employee relies on the data on Suspicious and unusual transactions issued by the Financial Intelligence Unit and the features described in clause 14.7 of this Procedure.

17 NOTIFICATION OBLIGATION IN CASE OF SUSPICION OF MONEY LAUNDERING AND TERRORIST FINANCING

17.1 If, in the course of his or her economic or professional activities, official activities or the provision of official services, an Employee identifies activities or circumstances the characteristics of which indicate the use of proceeds of crime, terrorist financing or related crimes or attempts to do so, or suspects that is Money Laundering or Terrorist Financing or committing related crimes, he is obliged to notify the Contact Person immediately.

17.2 The contact person is obliged to notify the Financial Intelligence Unit via the online form of the Financial Intelligence Unit or the *X-Tee* environment of the Financial Intelligence Unit immediately but not later than within two working days after the identification of activities or circumstances or the occurrence of suspicion. The notification shall be accompanied by the data used to establish the identity of the person and to verify the information provided and, if available, copies of the documents.

17.3 The relevant notice shall be submitted by the Contact Person to the Financial Intelligence Unit also if the establishment of a Business Relationship, transaction, operation or provision of services is not performed and the Client fails to request the information

17.4 The Company shall notify the Financial Intelligence Unit immediately, but not later than two business days after the conclusion of the transaction, of any notified transaction where a financial obligation exceeding 32,000 euros or the equivalent in another currency is settled in cash, regardless of whether the transaction is made in one payment or several related payments. for a period of up to one year.

17.5 Upon request, the contact person shall immediately provide the FIU with all available information requested by the FIU.

17.6 If the Company suspects or knows that it is Money Laundering or Terrorist Financing or committing related crimes, the performance of a transaction or official act or the provision of official services shall be postponed until the notification is submitted to the Financial Intelligence Unit.

17.7 If the postponement of a transaction may cause significant damage, failure to do so is not possible or may prevent a potential perpetrator of Money Laundering or Terrorist Financing from being caught, the Contact Person shall immediately contact the FIU by telephone and coordinate further actions and then submit a notice to the FIU.

17.8 All Employees of the Company, regardless of their position, are prohibited from notifying the Client and / or the person, its Ultimate Beneficiary, representative or third party of the notice submitted to the FIU, the plan or submission of such notice and the injunction or the commencement of criminal proceedings.

17.9 The Company may notify the Customer and / or the person of the disposal or other restriction of the account set by the FIU after the precept issued by the FIU has been complied with.

18 IMPLEMENTATION OF INTERNATIONAL SANCTIONS

18.1 An international sanction is a foreign policy measure aimed at supporting the maintenance or restoration of peace, international security, democracy and the rule of law, respect for human rights and international law, or the pursuit of other United Nations or Common Foreign and Security Policy objectives.

18.2 An international sanction shall be imposed on 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 other legislation imposing obligations on Lithuania.

18.3 A financial sanction is an international sanction which:

18.3.1 is obliged to freeze the funds and economic resources of the subject of the international financial sanction;

18.3.2 the making available of funds and economic resources to the subject of a financial sanction is prohibited;

18.3.3 the granting of loans and credits is prohibited under the conditions prescribed by the legislation implementing the international sanction;

18.3.4 the opening and use of a deposit, payment, security or other account is prohibited under the conditions prescribed in the legislation implementing the international sanction;

18.3.5 securities transactions are prohibited under the conditions prescribed in the legislation implementing the international sanction;

18.3.6 the conclusion of an insurance contract under the conditions prescribed in the legislation implementing the international sanction is prohibited;

18.3.7 investment is prohibited under the conditions prescribed by the legislation implementing the international sanction;

18.3.8 it is prohibited to enter into or continue a business relationship, advise or provide other financial services related to the activities listed above under the conditions prescribed by the legislation implementing the international sanction.

18.4 Upon entry into force, amendment or termination of the Financial Sanction, the Company shall check whether the person in its business relationship or planning to do so is the Subject of the Financial Sanction.

If the Company identifies the Subject of the Financial Sanction or that a transaction or act planned or performed by it violates the Financial Sanction, the Company shall apply the Financial Sanction (i.e., suspend the transactions) and immediately notify the Financial Intelligence Unit.

18.5 The Employee shall regularly check the Customer's data against the lists of international sanctions and https://namescan.io/FreeSanctionsCheck.aspx, https://www.sanctionsmap.eu/#/main or on the website of the Financial Intelligence Unit https during the independent inspections. Or using an information technology solution developed by the Company. The results of the inspections must be printed out on the date of the inspection and signed by the inspector. The respective document is archived at the Client's documents in accordance with the requirements for archiving the client's data.

18.6 If the Company doubts whether a person in its business relationship or planning to do so is the subject of a financial sanction or whether a transaction or act planned or performed by it violates the Financial Sanction, the Company shall apply the Financial Sanction and the Employee shall apply the following due diligence measures:

18.6.1 Collect additional information as to whether the person with whom it intends to do business or is planning to do so is in breach of the Financial Sanction or verifies it on the basis of additional documents, data or information from a reliable and independent source;

18.6.2 Collects additional information about the purpose and nature of the business relationship, transaction or operation and verifies it on the basis of additional documents, data or information from a reliable and independent source.

18.7 If, as a result of the application of due diligence measures, the Company identifies the Financial Sanction Entity or that a transaction or act planned or performed by it violates the Financial Sanctions or the additional information obtained during the application of due diligence.

19 MODEL FOR DETERMINING THE RISKS OF MONEY LAUNDERING AND TERRORIST FINANCING RELATED TO THE CLIENT AND ITS ACTIVITIES

19.1 The Company must recognize, assess and understand the risks related to Money Laundering and Terrorist Financing and the established International Sanctions in the activities of its Clients and apply measures to mitigate these risks.

19.2 The measures applied must be in accordance with the levels of risk assigned to the Clients. In taking a risk-based approach, the Company is required to assess the likelihood that risks will materialize and the consequences of materializing them. When assessing the probability, the possibility of the occurrence of the respective circumstances must be taken into account, including the possible dangers that may affect the activities of both the Client and the Company, and the possibility that the probability of the occurrence of this hazard increases.

19.3 The company is obliged to prepare a risk assessment in order to identify, assess and analyse the risks related to its activities. The steps taken to identify, assess and analyse risks must be proportionate to the nature, scale and complexity of the Company's business and professional activities.

19.4 This model for identifying and managing the risks related to the Client and its activities has been developed to implement the obligations arising from § 14 of the AML/CTF Law in accordance with the general regulations of the Money Market Act, the RSanS EU) 2015/849 and includes a model for identifying and managing the risks associated with the client and its activities and for determining the client's risk profile;

The following risk scale is used in this model:

A - low risk (1 risk point)

there is no risk factor with an impact in any of the risk categories and the Client and the Client's activities are transparent and do not deviate from the activities of a reasonable and average person, there is no doubt that the risk factors could lead to the realization of the risk of Money Laundering or Terrorist Financing.

B - medium risk (2 risk points)

there are one or more risk factors in the risk category that differ from the activities of a person operating in the same field of activity, but the activities are still transparent, and there is no doubt that the risk factors together could lead to the realization of the risk of Money Laundering or Terrorist Financing.

C - high risk (3 risk points)

there is one or more characteristics in the risk category that, in combination, call into question the person and make the activity transparent, which makes the person different from a person operating in the same field of activity, and at least the realization of Money Laundering or Terrorist Financing is possible.

19.5 The company must take all due diligence measures. The extent of implementation of the measures depends on the nature of the specific business relationship or transaction or the degree of risk of the person participating in the transaction or official act, including the principle of “know your customer”. When determining and furnishing the risk levels of a customer or a person participating in a transaction, the Company must take into account, inter alia, the following risk categories:

I. CUSTOMER RISK

1. RISK RELATED TO THE LEGAL NATURE OF THE CLIENT AND THE IDENTIFICATION OF THE ULTIMATE BENEFICIARIES

A- Low risk is assigned when the Client is:

- A company listed on a regulated market which is subject to disclosure obligations which impose requirements to ensure adequate transparency of the beneficial owner;
- A legal person in public law established in Lithuania;
- A government agency of Lithuania or a Contracting State of the European Economic Area or another institution performing public functions;
- An agency of the European Union;
- A credit institution acting on its own behalf, a credit institution or a financial institution located in a Contracting State of the European Economic Area or in a third country which is subject to requirements equivalent to those of Directive (EU) 2015/849 of the European Parliament and of the Council subject to national supervision;

B - Medium risk is assigned when the customer is:

- A natural person
- A company with a solid and transparent structure and data on the management bodies and actual beneficiaries (OÜ, AS, UÜ, TÜ, incl. foreign analogues of the mentioned company forms), which is not listed on the market;
- Non-profit association (NGO);

C - High risk is assigned when:

- The actual beneficiary of the natural person is a third party;
- The Client is a legal entity of any form, the structure of the governing bodies and / or the Actual Beneficiaries is incomprehensible and the said data is identified on the basis of the statements of the Client's representative and / or internal or non-public documents provided by the Client;
- The Client is a legal entity of any form, the structure of the management bodies and / or actual beneficiaries of which is incomprehensible, and the said data cannot be verified, incl.
- The client company or its related company has shareholders or bearer shares;
- The ownership structure of the client company seems unusual or too complex for the company to operate.
- The client is a foundation, partnership, trust fund or contractual fund;
- He is a person registered in a low-tax area.
- The customer is subject to the EU or UN sanctions.

2. RISK ASSOCIATED WITH COUNTRIES OR GEOGRAPHICAL AREAS OR JURISDICTIONS

A - Low risk is assigned when:

- The Client is from or has his or her residence or seat (hereinafter seat) in the Czech Republic;
- The Client is located in another country of the European Union or the European Economic Area;
- The client is domiciled in third countries equivalent to the Common Position adopted by the European Union, which include Australia, Brazil, Canada, Hong Kong, India, Japan, South Korea, Mexico, Singapore, Switzerland, South Africa, USA;

B - Medium risk is assigned when the client is located in a third country not mentioned above, except in a third country with a high risk;

C - The assessment of **high risk** factors shall take into account, in particular, the fact that the customer, party to the transaction or the transaction itself is related to a country or jurisdiction, unless there is no money laundering according to reliable sources such as peer reviews, detailed evaluation reports or published follow-up reports. and effective systems to prevent terrorist financing.

According to the Delegated Regulation (EU) 2016/1675 of the European Commission, third high-risk countries include Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, the Lao PDR, Syria, Uganda, Vanuatu, Yemen, Iran and the PRC. According to the FATF, the list of third high-risk countries is published at http://www.fatf-gafi.org/countries/#high-risk.

In addition, the relationship of the client, the person involved in the transaction or the transaction with the state or jurisdiction indicates a high risk:

- Where, according to reliable sources, the level of corruption or other criminal activity is significant. Data from the annual Corruption Perceptions Index (CPI) published by Transparency International (TI) is used to assess this fact, and high risk is characterized by a CPI score equal to or lower than 39. Data published by the CPI are available online at: https://en.wikipedia.org/wiki/Corruption_Perceptions_Index;
- subject to sanctions, embargoes or similar measures, such as those imposed by the European Union or the United Nations. A list of EU sanctions against countries is available online at https://sanctionsmap.eu; The UN Sanctions List is available online at https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list;
- Which finances or supports terrorism. These countries include the DPRK, Syria, Sudan and Iran and are defined in particular by data published by the United States Department of State, which is available online at: https://www.state.gov/j/ct/list/c14151.htm
- In whose territory terrorist organizations designated by the European Union or the United Nations operate. These countries include, in particular, Syria, Iraq, Libya, Sudan, Somalia, Nigeria, Pakistan, India, Lebanon, Palestine, Sri Lanka, the Philippines, Tajikistan, Uzbekistan and Yemen. The list of EU and UN-designated terrorist organizations is available online at: https://en.wikipedia.org/wiki/List_of_designated_terrorist_groups

3. RISK RELATED TO THE CUSTOMER'S BUSINESS AND THE PRODUCTS OR SERVICES OFFERED

A - Low risk is assigned when the client is a person engaged in ordinary and customary economic and professional activities and the client's cash flow or planned cash flow is significantly small and does not exceed 32,000 euros in a one-year period;

B - Normal risk is assigned when the client is a person engaged in ordinary and customary economic and professional activities and the client's cash turnover or planned cash flow exceeds 40,000 euros during a one-year period;

C - High risk is assigned when a business relationship operates in unusual circumstances, including complex and unusually large transactions and unusual transaction patterns, or the customer is a legal entity or other non-legal entity whose business does not have a reasonable, clear economic or legitimate purpose or Characteristic for business purposes or the client is engaged in or adjacent to his economic and professional activities, regardless of the size of turnover:

- Private or personal banking;
- Offering or brokering a product or transaction that may promote anonymity;
- Personal asset management;
- A company handling large amounts of cash;
- Currency exchange, conversion transactions;
- Providing a virtual currency exchange or virtual currency wallet service;
- Provision of gambling services (in a casino, via the internet or at sports competitions);
- Purchase and sale of gold (including scrap gold), other precious metals or precious stones;
- Purchase and sale of valuables;
- Providing online advertising;
- Offering innovative services;
- The formation, sale and management of companies;
- This is another area where there is a higher than usual risk of money laundering or terrorist financing;
- The customer provides services through non-traditional sales channels;
- There is a constant change of customers;
- A person's customer base has grown rapidly.

4. SETTLEMENT AND TRANSACTION RISK

A - Low risk is assigned when:

- A duration agreement has been entered into with the customer in written, electronic or written form;
- Payments to the company in the framework of a business relationship are received only through an account located in a credit institution registered in Lithuania or in a branch of a foreign credit institution established or domiciled in a European Economic Area country or third country where Directive (EU) 2015/849 requirements equivalent to those required;
- The total value of incoming and outgoing payments in commercial transactions does not exceed EUR 15 000 per year.

B- Medium risk is assigned when a customer uses to settle with the Company:

- A limited amount of cash not exceeding EUR 15 000 or the equivalent in another currency, whether the transaction is made in a single payment or in several interconnected payments over a period of up to one year;
- Uses for settlement a credit, financial institution, payment institution or tax system which is not located in a high-risk third country and which does not promote anonymity, which is reliable in its experience or from independent sources and carries out controls against money laundering and terrorist financing.

C - High risk is assigned when a client uses:

- A credit institution, financial institution, payment institution or tax system which promotes anonymity;
- A credit institution, financial institution, payment institution or tax system located in a high-risk third country;
- Settlement channels and accounts belonging to unknown or unrelated third parties;
- Large amounts of cash in excess of EUR 15 000 or the equivalent in another currency, whether the transaction is made in a single payment or in several interconnected payments over a period of up to one year.

5. CUSTOMER IDENTITY RISK

A - Low risk is assigned when:

- A natural person resident in the Czech Republic is identified while staying in the same place;
- A client who is a legal person entered in the commercial register of the Czech Republic, non-profit associations and foundations has been identified on the basis of original the documents provided for in the Agreement and, in the case of an authorized person, on the basis of a notarised or equivalent document certifying his or her authority, which has been legalized or certified by an apostille, unless otherwise provided by an international agreement.

B – Medium risk is assigned when:

- A foreign individual customer has been identified while staying in the same place on the basis of the original documents provided;
- A foreign legal person client has been identified on the basis of the original documents by verifying the identity of the representative on the basis of the said documents, or on the basis of a notarized equivalent, which is legalized or confirmed by a certificate replacing legalization (apostille), unless otherwise provided by an international agreement;
- A notarised or officially certified copy of the documents shall be verified of the identity of a natural or legal person.

C- High risk is assigned when:

- The identity or verification of the information provided has cast doubt on the veracity of the information provided or the authenticity of the documents or the identification of the beneficial owner;
- A business relationship or transaction which is established or initiated in a manner in which the client, his or her representative or a party to the transaction is not present and the application of the AML/CTF Law is not applied as a safeguard;
- Identity is established using other information from a reliable and independent source, including e-identification and e-transaction trust services, in which case at least two different sources shall be used to verify the data;
- The client is represented by a legal entity.

6. RISK ASSOCIATED WITH THE CHANNELS OF COMMUNICATION OR TRANSMISSION BETWEEN THE COMPANY AND THE CLIENT

A - Low risk is assigned when:

- The client is communicated through a communication or mediation channel agreed upon at the initiative of the business relationship or transaction or reliably changed during the business relationship;
- The products or services are delivered to the customer through a reliably modified transmission channel during the business relationship or at the initiative of the transaction;

B – Medium risk is assigned when:

- The Client is communicated through another temporary communication or mediation channel transmitted through an agreed communication or mediation channel on the initiative of the business relationship or transaction;
- The products or services are delivered to the customer through another temporary channel for the transmission of products or services via the communication or intermediation channel agreed upon at the initiative of the business relationship or transaction;

C - High risk is assigned when:

- The client is communicated through an accidental, unreliable or unusual communication or mediation channel;
- Products or services are delivered to the customer through an accidental, unreliable or unusual delivery channel;
- The existence and nature of a risk factor related to the service provider used to deliver the service or product sold;
- There is a significant distance between the customer's location and the destination of the service or goods sold.

19.6 Taking into account the above risk categories, the Company must determine the level of risk of the person involved in the transaction or the client, for example whether the client's money laundering or terrorist financing risk is low, normal or high or meets other risk levels assigned and used by the Company.

19.7 In order to determine the effect of each risk category, the company must assess the probability of the occurrence of risk factors in that risk category. The qualifying amount of the presence of risk factors that characterize a particular risk category may be used to determine whether a particular risk factor is "affected" or "non-affected" for a given person when a certain threshold is exceeded.

19.8 Certain guidelines for defining a low level of risk:

- The client's level of risk is generally low if there is no influential risk factor in any of the risk categories, so it can be argued that the client and his activities do not have the characteristics of a normal and transparent person, and there is no doubt that the client may increase money laundering and terrorism. the likelihood of funding.

- In situations where the application of due diligence is required by law and information about the customer and its beneficial owner is publicly available31, where the person's activities and transactions are consistent with the day-to-day business and the tax and behaviour of other similar customers, or where there are quantitative or other absolute restrictions, the Company may consider the customer's expected risk of money laundering or terrorist financing to be low.
- In a situation where at least one risk category qualifies as high, the degree of risk of money laundering or terrorist financing cannot generally be low. On the contrary, low risk does not necessarily mean that the client's activities cannot be linked to money laundering or terrorist financing at all.
- If the risk arising from the business relationship, the person or the party to the transaction is low based on the risk levels assigned to the party or the client and other conditions set out in the AML/CTF Law are met, the Company may apply due diligence but may not apply due diligence at all. In applying the simplified due diligence measure, the Company may determine the extent of compliance with the due diligence measure.

19.9 Certain guidelines for defining a high degree of risk:

- The client's level of risk is generally high if, when assessing the risk categories as a whole, there is a suspicion that the client's activities are not routine or transparent, including the existence of influential risk factors, which can be assumed to be high or significantly increased. The client's risk level is high even if it is required by a separate feature of the risk factor. However, a high risk does not necessarily mean that the customer is engaged in money laundering or terrorist financing.
- If the Company assesses the level of risk of a client or a person involved in a transaction as high, the Company must apply enhanced due diligence measures34 in order to properly manage the respective risks. At the same time, due diligence measures must be applied in accordance with the provisions of the AML/CTF Law.

19.10 The company should document the risk assessment, keep it up to date and make it available to the competent authorities as necessary.

20 CUSTOMER RISK IDENTIFICATION MODEL

This guide uses the table below to identify the client's level of risk, which includes the arithmetic method and formula used to determine the client's level of risk. This table shall be completed with the results of the customer analysis previously performed in accordance with this Annex (1 to 3 risk points shall be awarded for each aspect of risk analysed).

RISK CATEGORIES:

1. The risk associated with the legal nature of the customer and the identification of the beneficial owners;
2. Risk associated with countries or geographical areas or jurisdictions;
3. Risk related to the customer's field of activity and the products or services offered;
4. Risk related to settlement and transactions;
5. Risk related to the customer's identity;

6. The risk associated with the communication or transmission channels between the company and the customer.

TABLE:

	Low (1 point)	**Medium (2 points)**	**High (3 points)**	**Coefficient**	**Result**
1 risk cat.				2	

2 risk cat.				1	
3 risk cat.				2	
4 risk cat.				1	
5 risk cat.				1	
6 risk cat.				1	
The parameters for determining the client's risk levels are: A. Customer risk level is **low** if x <2 B. Customer risk level is **medium** if 2 ≤ x ≤ 2.75 C. Customer risk level is **high** if x> 2.75				**Average score (x):** **Customer risk level**	

NB! even if the average score of the client's level of risk indicates a low risk category, it cannot be a client with a low risk category where at least one of the categories is high risk. The client's overall risk category is high even if it is required by a separate risk factor.

ANNEX 1. SANCTION STATES

Afghanistan	AF
Bosnia and Herzegovina	BA
Guyana	GY
Iran	IR
Iraq	IQ
North- Korea	KP
Laos	LA
Ethiopia	ET
Pakistan	PK
Serbia	RS
Sri Lanka	LK
Syria	SY
Trinidad and Tobago	TT
Tunisia	TN
Uganda	UG
Vanuatu	VU
Yemen	YE

ANNEX 2: LOW TAX TERRITORIES

American Samoa	AS	Liechtenstein	LI
Andorra	AD	Macao SAR	MO
Anguilla	AI	Maldives	MV
Antigua and Barbuda	AG	Marshall Islands	MH
Aruba	AW	Mauritius	MR
Bahamas	BS	Nauru	NR
Barbados	BB	Niue	NU
Belize	BZ	Palau	PW
Bermuda	BM	Panama	PA
British Virgin Islands	VG	Saint Lucia	LC
Cabo Verde	CV	Saint Kitts and Nevis	KN
Cayman Islands	KY	Saint Vincent and the Grenadines	VC
Cook Islands	CK	San Marino	SM
Curaçao	CW	Seychelles	SC
Faroe Islands	FO	Trinidad and Tobago	TT
Guernsey	CG	Turks and Caicos Islands	TC
Guyana	GY	United Arab Emirates	AE
Isle of Man	IM	Uruguay	UY
Hong Kong SAR	HK	US Virgin Islands	VI
Jersey	JE	Vanuatu	VU

Labuan Island	-	

ANNEX 3: OTHER HIGH RISK AREAS

Albania	AL	Malaysia	MY
Bahrain	BH	Morocco	MA
Botswana	BW	Namibia	NA
Dominica	DM	New Caledonia	NC
Ethiopia	ET	Oman	OM
Fiji	FJ	Qatar	QA
Grenada	GD	Samoa	WS
Jamaica	JM	Sri Lanka	LK
Jordan	JO	Swaziland	SZ
Laos	LA	Tunisia	TN
		Uganda	UG

2 RISK ASSESSMENT RELATED TO MONEY LAUNDERING AND TERRORISM FINANCING AND COMPANY RISK

1 PURPOSE

1.1 The purpose of the Risk Assessment and Risk Appetite Procedure is:

- Identify, assess and analyse the Money Laundering or Terrorist Financing risks related to the Company's operations;
- Determine the risks related to the Clients;
- Identify risks associated with countries or different jurisdictions;
- Identify the risks associated with products and services;
- Identify the risks associated with communication or channels of mediation;
- Identify the risks associated with the transmission channels for transactions;
- Establish risk management measures to be implemented;
- Determine the levels and types of risks that the Company is prepared to take;
- Designate the responsible persons.

2 RESPONSIBILITY

2.1 The Management Board is responsible for compliance with the requirements and compliance therewith.

2.2 The procedure is mandatory for all Managers and Employees.

3 GENERAL

3.1 The Company offers the Clients a virtual currency service.

3.2 The provision of the Service involves various risks and potential losses related to Money Laundering and Terrorist Financing, and the Company must take appropriate measures to identify, assess, analyse and mitigate them.

3.3 In compiling the procedure, the specifics of the Service provided by the Company, the legislation applicable to the Company, the Financial Intelligence Unit and other instructions applicable to the Company have been taken into account.

4 RISKS

4.1 Given the nature, scale and complexity of its operations, the Company considers the following risks to be significant and assesses in particular:

4.1.1 Risk related to the Clients: the risk that a change in the background or behaviour of the Clients will cause a loss or reduce the income;

4.1.2 Country or Jurisdictional Risk: The risk that an increase in the Corruption Perception Index of the Clients' countries of origin and destination, the risk of terrorism and drug trafficking, or the imposition of international financial sanctions will expose reputational and legal risks and reduce projected revenue;

4.1.3 Product-Related Risk: The risk that the Service provided will be used in the Money Laundering and Deployment phases of the Money Laundering Cycle or in the Financing of Terrorism. This carries reputational and legal risks.

4.1.4 Channel risk: the risk that an electronic solution for the provision of a service or persons associated with the Company will use professional inside information to enable Money Laundering or Terrorist Financing. This carries the risk of loss of reputation, legal, planned income, capital or the Company's license.

5 RISK ANALYSIS

5.1 The Company regularly analyses and evaluates various possible risk scenarios arising from internal and external risk factors in its operations and in the development of its business strategy.

5.2 The Management Board has approved the Notes to the Internal Rules, which set out the Risk Assessment and Risk Appetite related to the Company's Money Laundering and Terrorist Financing (Note 4. Quan2um OÜ Risk Assessment and Risk Appetite related to Money Laundering and Terrorism Financing)

5.3 In the course of the risk analysis of the main business processes of the company, the risks mapped in cooperation with the Management Board, the Employees and, if necessary, the internal auditor are assessed. Particular attention will be paid to the risk related to Terrorist Financing, which in the opinion of the Company is considerably high in the provision of the Service.

5.4 The Management Board, the Contact Person and, if necessary, the internal auditor shall assess both actual and potential risks, collect relevant information and seek opportunities to implement the conclusions reached during the risk analysis.

6 RISK ASSESSMENT

6.1 The likelihood and frequency of money laundering and terrorist financing risk is assessed as follows:

Probability	Frequency	Level
<5%	One case in the period of 3 years	Very low
6-20%	One case in the period of 1 year	Low
21-40%	One case in the period of 6 months	Medium
41-60%	One case in the period of 3 months	High
>60%	One case in the period of 1 month	Very high

6.2 The effects of the risks are assessed as follows:

Level	Impact
Low	the occurrence of risk does not interfere with the achievement of the Company's business objectives
Medium	when the risk arises, the Company's activities and achievement of goals are somewhat disrupted, but the goals are achievable and additional resources are needed to a small extent
High	when the risk arises, the activities and the achievement of the goals are significantly disrupted, a significant amount of additional resources are needed to achieve the goals
Very high	it is not possible to continue activities and / or achieve goals if the risk arises, the elimination of damage requires significant resources

6.3 The risks of Money Laundering and Terrorist Financing are divided into two categories based on their probability, frequency and impact:

6.3.1 Larger category of risks:

6.3.1.1 risks with a high or very high probability of occurrence and a very high or high impact;

6.3.1.2 risks with a very low, low or medium probability of occurrence and a very high or high impact;

6.3.2 Risks of a lower category:

6.3.2.1 risks with a medium, low or very low probability of occurrence and a medium or low impact.

6.3.2.2 risks with a high or very high probability of occurrence and a medium or low impact.

6.4 The risks of Money Laundering and Terrorist Financing are assessed continuously, and the Contact Person submits an overview to the Management Board as necessary, but at least once a quarter.

7 MANAGING THE RISKS OF MONEY LAUNDERING AND TERRORISM FINANCING

7.1 The company takes a conservative approach to its business.

7.2 In order to mitigate the risks of Money Laundering and Terrorist Financing, the Company develops and establishes Internal Rules that comply with the requirements of legislation and cover all the Company's processes and update them as necessary, but at least once a year.

7.3 The Company shall establish a comprehensive system of continuous internal control with the Internal Rules, including clear responsibilities, subordination and reporting chains for Managers and Employees.

7.4 The Company's organizational structure is based on the principle of separation of functions, which helps to ensure impartiality in assuming obligations for and on behalf of the Company, reflecting the Services in the Company's accounts and reports, managing the Company's risks and performing internal control. No Employee has the opportunity to control the entire process or a significant part of it alone (partly because a large part of the process is automated).

7.5 The organization the organizational structure of risk management related to Money Laundering and Terrorist Financing is based on the principles of the internationally recognized Three Lines of Defence, where:

7.5.1 The First Line of Defence, i.e., the business area, is responsible for risk-taking and day-to-day management;

7.5.2 Second Line of Defence or compliance check is responsible for the development and updating of risk management methodologies and reporting

7.5.3 The Third Line of Defence, i.e., internal audit, performs independent supervision over the entire activities of the organization and reports to the Management Board or directly to the owners of the Paying Authority.

7.6 The Company selects as its Employees competent persons who know the specifics of the target market.
Special attention is paid to the training of employees, including the introduction of the Internal Rules.

7.7 The Company enters into cooperation agreements only with correct and well-known cooperation partners who have the necessary permits, technical systems and resources for the provision of a specific service and who are able to take into account the increased requirements established for the Company. The partners are thoroughly inspected to ensure that they comply with the requirements of the Company listed above. If necessary, a service contract will be entered into in accordance with the procedure for the transfer of the Company's activities.

7.8 The company's business is based on customer relationships. The principle of “knowing your customer” is central to the provision of services, when the extent of knowing the Customer must correspond to the results of the Risk Assessment. The Company assesses the profile of the Clients and the associated risks of Money Laundering and Terrorist Financing when concluding Client Agreements and on an ongoing basis. The Company does not provide the Services to persons with whom a Customer Agreement has not been entered into and whose identity has not been properly established.

7.9 The Company shall store and maintain all required data on the Clients and the Instructions given by them and shall ensure the availability of such data to the supervisory authorities.

7.10 In providing the Service, the Company shall use only such information technology solutions that enable the screening of the parties to the mediated payments against Money Laundering, Transactions with Suspected Terrorist Financing and Lists of Financial Sanctions.

7.11 The company develops and implements IT solutions to detect various risk indicators during regular monitoring.

7.12 The Company shall provide the Regulator with compliance checks or risk analysis (s) and / or reviews to the Management Board as soon as practicable if significant deficiencies are identified in the measures and activities taken to prevent money laundering and terrorist financing.