XAZUR TECHNOLOGIES EUROPE, UAB

Internal rules

Table of Contents

1. DEFINITIONS

AML/CTF Law	Law on the Prevention of Money Laundering and Terrorist Financing of Lithuania.
Board Member	Member of the XAZUR TECHNOLOGIES EUROPE, UAB Management Board.
Business Continuity	The ability of a company to conduct business without interruption.
Business Continuity Plan	Written business continuity management plan for the restoration and continuation of business operations in the event of the realization of business interruption risks identified during the risk analysis.
Business-Wide Risk assessment	Continuous management activities of the Company, in the course of which the Company's potential business risks, their impact on the provision of the Service are assessed and as part of which the Company's Business Continuity Plan is prepared.
Company	XAZUR TECHNOLOGIES EUROPE, UAB, registry code <305945076>
Contact person	A member of the Management Board of the Company or a person appointed by the Management Board who is responsible for reporting to the Financial Intelligence Unit, complying with precepts and applying international financial sanctions on the basis of the Company's Prevention of Money Laundering and Terrorist Financing and the Application of Financial Sanctions.
Customer	A natural or legal person with whom the Company has entered into a Customer Agreement or is negotiating to enter into a Customer Agreement.
Customer Agreement	An agreement entered into between the Company and the Customer, on the basis of which the Company provides the Customer with a virtual currency service and the Customer pays a fee for it.
Customer Environment	An Internet environment accessible via the Company's website and mobile application, which enables the Customer to communicate with the Company, including concluding a Customer Agreement, submitting Transactions, etc.
Customer relationship	The business relationship between the Company and the Customer, established upon concluding a Customer Agreement.
Employee	A natural person who works for the company on the basis of an employment or similar contract.
Financial Intelligence Unit (the FIU)	An independent structural unit of the Police and Border Guard Board, the main task of which is to prevent money laundering and terrorist financing in Lithuania.
Financial sanction	A financial sanction is an international sanction by which the subject of the sanction, in whole or in part, is prevented from using and disposing of his or her funds and economic resources or placing them in his or her possession in accordance with the provisions of the International Sanctions Act.
Internal rules	The Company's rules of procedure and internal control rules established in accordance with the Republic of Lithuania Law on the Prevention of Money Laundering and Terrorist Financing
Management board	XAZUR TECHNOLOGIES EUROPE, UAB Management Board.
Money laundering	Assets derived from or in lieu of money laundering:

	1) conversion or transfer, if it is known that such property has been obtained from criminal activity or participation therein, with the purpose of concealing the property of illegal origin or to assist a person involved in a criminal activity in order to avoid the legal consequences of his or her actions; 2) acquisition, possession or use, if upon receipt it is known that it has been obtained from criminal activity or participation therein; 3) concealment of the true nature, origin, location, manner of disposal, transfer or ownership, or concealment of other rights related to property, or if it is known that such property has been obtained from criminal activity or participation therein. Money laundering also includes participation in, association with, attempts to commit, aiding, abetting, facilitating or counseling the commission of any of the foregoing activities. Money laundering also occurs if: 1) the criminal activity, as a result of which the property used for money laundering was obtained, took place in the territory of another state; 2) the details of the criminal activity which resulted in the acquisition of the property used for money laundering have not been established.
Personal data	Any data relating to an individual through which that individual may be identified directly and/or indirectly.
Politically Exposed Person (PEP)	A natural person who performs and / or has performed prominent public functions in Lithuania, in another Member State of the European Economic Area, in third countries or at an institution of the European Union, and family members and close associates of such person. A person who has not performed essential functions of public authority for at least one year or family members and close associates of such a person by the date of the transaction shall not be deemed to be a politically exposed person. The prominent public functions are: - the Head of State; - the Head of Government; - the Minister, the Deputy Minister or the Assistant Minister;

	- a Member of Parliament or a member of a legislative body similar to Parliament; - a member of the governing body of a political party; - Member of the High Court and the Supreme Court; - Member of the Supervisory Board of the National Audit Office and the Central Bank; - the Chancellor of Justice; - Ambassador - Envoy - a high-ranking officer in the Defense Forces; - a member of the management board and administrative or supervisory body of a state-owned company - the head of an international organization, a deputy head and a member of the governing body, or a person performing equivalent duties, who is not a middle or lower-ranking official.
Price list	The price list of the services offered by the Company in accordance with the decision of the Management Board and published in the Customer Environment.
Procedure	Reference to the relevant Internal Rules.
Processing of personal data	Any act performed with personal data, including the collection, storage, modification and disclosure of personal data, the provision of access, the retrieval of personal data, the use, transfer, cross-use, aggregation, retention, deletion or destruction of personal data, or any of the above; the manner in which they are carried out and the means employed.
Processor of personal data	The natural or legal person, public authority, agency or other body of the controller which, solely or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or national law, the controller or the specific criteria for its designation may be laid down in Union or national law. - The processor responsible for the employee's personal data is the Company; - The processor responsible for the customer's personal data is the Company. "Processor" means any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

	- The authorized processor of the employee's personal data is the undertakings providing the support service to the employer or the structural units of the enterprise (e.g. the structural units providing personnel and accounting services, as well as the legal service, real estate, risk management and internal audit service, etc.). The authorized processor of the customer's personal data may be, for example, the Company's server hosting service provider.
Risk	A set of types and levels of risks related to the Company's Money Laundering and Terrorist Financing that meets the requirements of AML/CTF Law and is approved by the Management Board in the course of its operations and is approved by the Management Board.
Risk Assessment	Assessment of risks related to Money Laundering and Terrorist Financing prepared by the Company and approved by the Management Board in accordance with the requirements of § 14 of AML/CTF Law.
Service	The actual natural person of the Beneficial Owner who, by taking advantage of his or her influence, performs the transaction or act or otherwise has control over the transaction, act or other person and in whose interest, for whose benefit or at the expense the transaction or act is performed. In the case of a company, the beneficial owner shall be a natural person who: 1) ultimately owns shares in the company or exercises ultimate control over the management of the company, including by owning more than 25% of the shares, direct or indirect ownership or control, including in the form of bearer shares; 2) is a beneficiary of the property of a legal person, partnership or other such legal entity engaged in the management or distribution of property: - at least 25% plus one share per share as determined in advance; - to an extent not specified in advance and in whose interests a principal legal person, partnership or other similar legal arrangement is set up or operates; 3) controls to a significant extent the assets of a legal person, partnership or other such legal entity to the extent of at least 25% plus one share; If, after all the means of identification have been exhausted, the person described in the preceding paragraphs cannot be identified and there is no doubt that such a person still exists, or if there is any doubt as to whether the identified person is a beneficial owner, the beneficial

	owner shall be a natural person who is a member of the company's senior management board.
Significant function	The principal line of business and related services that pose a significant source of revenue or profit for the Company (unless the Company has determined that failure or improper performance of such a delegated function will not impair the continuity of the principal line of business function).
Special categories of personal data	Data concerning political, religious and philosophical views, information on the membership of legal persons in the trade union registered pursuant to the procedure prescribed by law; data describing ethnic origin and racial origin; data on health status or disability; genetic and biometric data; data on sexual life and orientation; information concerning the commission or commission of an offense before a public court hearing or a decision on the offense or the termination of the proceedings on the matter.
Subject of the financial sanction	A state, territory, territorial unit, regime, organization, association, group, natural or legal person, agency, partnership or any other entity directly mentioned in the instrument imposing or enforcing an international sanction and subject to the measures provided for in the instrument imposing the international sanction.
Terrorist financing	Financing and support of a terrorist offense and activities directed at its commission and travel for terrorist purposes within the meaning of §§ 252^1 (1) and (2) of the Criminal Code.
Third party	A person who is not a Company or a Customer.
User Account	The Customer's personal user account, which allows the Customer to access the Customer Environment via the Company's website and mobile application.

2. GENERAL PART OF THE INTERNAL RULES

1 OBJECTIVES OF ESTABLISHING INTERNAL RULES

The business activities of the company as a provider of virtual currency cash exchange and virtual currency wallet service provider are primarily related to the handling and storage of digitally presented values. The provision of a virtual currency for money exchange and virtual currency wallet service primarily requires the use of new and evolving technologies, which may involve the implementation of new or non-traditional sales channels in the Company's business.

The vast majority of virtual currencies are cryptocurrency and related tokens, built on a new and rapidly evolving blockchain technology and a distributed database that is updated through a mathematical consensus. algorithm.

The Management Board evaluates the activities of the Company providing virtual currency cash exchange services and virtual currency wallet services as a higher-than-usual area of activity within the meaning of AML/CTF Law. This assessment stems in particular from the following factors:

1) Blockchain technology is a new and evolving phenomenon, so the mechanisms and algorithms for its occurrence, existence, transfer and trading are not constant and may be too complex and incomprehensible. This encourages the involvement and use of virtual currencies, including cryptocurrency, in various fraudulent schemes and scams;

2) Blockchain technology promotes anonymity (cryptocurrency wallet addresses are not personalized and are expected to be used in large quantities), which may contribute to the use of virtual currencies, including cryptocurrency, in money laundering, tax evasion, terrorist financing or criminal schemes;

3) Block chain technology is based on a P2P network and is not regulated by any central organization that may facilitate the manipulation of the value of virtual currencies, including cryptocurrencies.

1.1 The Company shall establish Internal Rules governing the activities of Managers and Employees to ensure that:

1.1.1. The activities of the Company comply with the relevant legislation, the instructions and precepts of the supervisory authorities and the decisions of the governing bodies of the Company;

1.1.2. It is clear to Managers and Employees how the Services are provided and related operations are performed within the Company and what are the roles and responsibilities of each Manager and Employee in order to ensure that the services provided by the Company are consistent and of high quality and in accordance with high standards of diligence;

1.1.3. The Company's internal reporting lines, reporting chains and internal controls are unambiguous, transparent and effective to ensure that Managers and Employees have a clear understanding of their rights and responsibilities and are monitored systematically, consistently and effectively to prevent and promptly address service issues. thereby ensuring the high quality of the Services provided by the Company and compliance with legislation;

1.1.4. If necessary, the Company is able to provide an overview of its activities quickly and in accordance with the requirements to all supervisory authorities (incl. the Financial Intelligence Unit), thus ensuring that the required supervision of the Company can be performed.

2 BASIS FOR ESTABLISHING INTERNAL RULES

2.1. The basis for establishing internal rules is derived primarily from the AML/CTF Law.

2.2. The internal legislation is based in particular (but not exclusively) on the following legislation:

2.2.1. Law on the Prevention of Money Laundering and Terrorist Financing of Lithuania. (hereinafter: AML/CTF Law);

2.2.2. the Civil Code;

2.2.3. Law of Republic of Lithuania on Legal Protection of Personal Data (hereinafter: DPA);

2.2.4. the Law on Consumer Protection;

2.2.5. the Accounting Law;

2.2.6. the Law on the Audit of Financial Statements;

2.2.7. International Sanctions Act (hereinafter: ISA).

3 COMPOSITION OF INTERNAL RULES

3.1. Pursuant to the specifics of the Company's economic activities and applicable legislation, the Internal Rules consist of the following procedures:

1. DEFINITIONS
2. GENERAL PART OF THE INTERNAL RULES
3. PROVISION OF SERVICES
4. EXECUTION OF TRANSACTIONS

5. OUTSOURCING PROCEDURE
6. PROCEDURES FOR THE FINANCING OF MONEY LAUNDERING AND TERRORISM AND INTERNATIONAL SANCTIONS
7. RISK ASSESSMENT RELATED TO MONEY LAUNDERING AND TERRORISM FINANCING AND COMPANY RISK
8. SECURITY AND INFORMATION SYSTEMS OF INFORMATION TECHNOLOGY SYSTEMS INSPECTION PROCEDURES
9. MAINTENANCE OF DATABASES, DATA PROCESSING AND INTERNAL INFORMATION AND PROCEDURE FOR THE MOVEMENT OF DOCUMENTS
10. DUTIES, SUBSIDIARIES, REPORTING AND DUTIES OF MANAGERS AND STAFF PROCEDURE FOR DELEGATION
11. PROCEDURE FOR THE OPERATION OF THE INTERNAL CONTROL SYSTEM
12. ENSURING RISK MANAGEMENT AND BUSINESS CONTINUITY PROCEDURE
13. INTERNAL ACCOUNTING RULES
14. PRINCIPLES OF PROTECTION AND CUSTODY OF CLIENT'S ASSETS
15. PROCEDURE FOR THE COLLECTION OF STATISTICS ON PERFORMANCE, TRANSACTIONS AND FRAUD
16. INVESTMENT POLICY
17. PROCEDURE FOR PROCESSING PERSONAL DATA

4 ESTABLISHMENT AND AMENDMENT OF INTERNAL RULES

4.1. The new version of the Internal Rules and each of the procedures forming part thereof shall be approved by a decision of the Management Board and a corresponding reference shall also be made to the Internal Rules and each new version of the procedure forming part thereof.

4.2. Internal rules are reviewed and updated at least once a year, as well as if necessary due to problems in servicing the Customer, changes in the Company's operations, changes in legislation regulating the Company's activities or a proposal of the supervisory authority. The Head of Compliance checks the changes in the legislation regulating the activities of the Company and, if necessary, makes a proposal to amend the Internal Rules taking into account the results of the check.

4.3. Any Manager and Employee may also propose to the Management Board to amend the internal rules. The Management Board will decide on the response to the proposal, if necessary in consultation with the Company's legal advisor and the person responsible for compliance with the requirements of the Internal Rules referred to in the proposal.

4.4. The Management Board or a person appointed by the latter shall immediately notify all Managers and Employees of the established Internal Rules and their amendments.

4.5. The Manager or Employee appointed as the person responsible for the internal rules or the procedure resulting therefrom shall be responsible for introducing the amendments to the Managers and Employees

arising from the new version of the Internal Rules and for receiving the latter's written confirmation thereof.

4.6. The established Internal Rules and their amendments are binding on the Company and all Managers and Employees as of their establishment and notification.

4.7. The Management Board shall keep in writing or in a form that can be reproduced in writing all versions of the Internal Rules and the procedures forming part thereof and the decisions of the Management Board approving them.

4.8. The Management Board or an employee appointed by the latter shall submit new versions of the Internal Rules and the procedures forming part thereof to the Financial Intelligence Unit in accordance with the requirements arising from legislation.

3. PROVISION OF SERVICES

1 PURPOSE

1.1 The purpose of the procedure is to determine:

- the procedure for establishing a Customer Relationship and concluding a Customer Agreement, including the procedure for creating and personalizing a User Account and the grounds for refusing to establish a Customer Relationship;

- the grounds and procedure for the termination, termination and suspension of the Customer Agreement;

- Conditions and procedure for submission and approval of instructions;

- Conditions and procedures for receiving, accepting and executing instructions;

- Procedure for providing information to the Client on the execution of instructions;

- procedures for dealing with non-compliant or incorrectly executed Instructions;

- the procedure for withholding fees and other expenses;

- Compliance with the requirements of the Procedure and proper compliance with the Procedure by the Managers and Employees

- the persons responsible for inspection.

2 RESPONSIBILITY

2.1 The Management Board is responsible for checking the correspondence of the procedure to the legal requirements and proper compliance with them.

2.2 The procedure is mandatory for all Managers and Employees.

3 CUSTOMER RELATIONSHIP

3.1 The Company has the right to decide with whom to establish a Customer Relationship and enter into a Customer Agreement. When making a decision, the Company fully considers all the circumstances that

may lead to the Company refusing to establish a Customer Relationship and enter into a Customer Agreement.

3.2 In order to establish a customer relationship, the Customer must perform the following actions, in the following order or in another order permitted by the Company:

3.2.1 create a personal User Account in accordance with clause 4.3 of the Procedure;

3.2.2 when using himself or herself and the representative, also establish the identity of his or her representative and the basis for the right of representation of the representative in accordance with clauses 4.4 and 4.5 of the Procedure;

3.2.3 enter into a Customer Agreement in accordance with clause 4.6 of the Procedure;

3.2.4 personalize the User Account in accordance with clause 4.7 of the Procedure.

3.3 The Customer creates a User Account in the Customer Environment using an ID card, Mobile ID, Google Account and Authenticator, Facebook account or similar tool, which allows to uniquely identify the Customer or the User Account is created by the Company in the same place as the Customer.

3.4 The identity of the Client and, if necessary, his / her representative and the basis of the representative's right of representation shall be established in accordance with the Company's Procedure for the Prevention of Money Laundering and Terrorist Financing and the Application of Financial Sanctions (Procedure 6).

3.5 Based on the information about the Customer submitted by the Customer upon establishment of the Customer Relationship and other publicly available information to the Company, the Company collects additional information about the Customer in accordance with its internal rules and legislation and requires the Customer to provide additional information and documents.

3.6 After the Client and his / her representative has established the identity of the Client's representative and the basis for the right of representation, the Client shall be provided with the terms and conditions of the Client Agreement, displaying them in the Client Environment, offering the Client the option to download the Client Agreement. The Company will not allow the Customer to continue the process of establishing a Customer Relationship until the Customer has confirmed that he or she agrees to the terms and conditions of the Customer Agreement and the conclusion of the Customer Agreement. The terms and conditions of the client agreement shall be established by a resolution of the Management Board based on the requirements provided by legislation.

3.7 If the Client Agreement is entered into by the Employee in the same place as the Client, the Client confirms his / her acceptance of the terms and conditions of the Client Agreement by signing the Client Agreement on paper. The Employee, in turn, confirms with his / her signature the identification of the

Customer and the conclusion of the Customer Agreement with the Customer in accordance with the Company's internal rules and legislation and activates the User Account.

3.8 The Company refuses to establish a Customer Relationship:

3.8.1 a natural person or a representative of a legal person who does not have the document required for identification;

3.8.2 a natural person or a legal person whose address of residence is located in the countries listed in Annex 1, Annex 2 and Annex 3 to the Procedure for Financing Money Laundering and Terrorism and the Preparation of International Sanctions;

3.8.3 a natural person or a representative of a legal person who is not at least 18 years old;

3.8.4 a legal person registered or having its registered office in a country or territory listed in Annex 1, Annex 2 and Annex 3 to Procedure 6;

3.8.5 a trust, partnership or other such contractual legal entity;

3.8.6 a person who does not confirm that he is the Actual Beneficiary when using the Company's services;

3.8.7 a person who does not confirm that he is not and that his representative and the Actual Beneficiary is not a Person with a State Background;

3.8.8 a person who is not open in his / her own name in a credit institution or financial institution located in a Contracting State of the European Economic Area or in a third country that is subject to national supervision in a country equivalent to Directive (EU) 2015/849;

3.8.9 a person who does not have an activity license to operate as a credit or financial institution, but whose main and permanent economic activity through the Company or through the Company is similar to or corresponds to the provision of financial services requiring an activity license;

3.8.10 a person in respect of whom money laundering or Terrorist Financing is suspected or who is or has been involved in traditional sources of income of organized crime;

3.8.11 a person who is entered in the List of Subjects of a Financial Sanction;

3.8.12 a person who does not provide the Company with the necessary information on the purpose of the transaction;

3.8.13 intentionally or due to gross negligence provided incorrect or incomplete information or documents to the Company or refuses to provide the Company with the information or

documents required pursuant to the Customer Agreement or legislation (incl. Prevents the application of due diligence measures).

3.9 The Company has the right to refuse to establish a Customer Relationship with a person who is:

3.9.1 (has been) significantly or repeatedly delayed in performing its obligations to the Company; and / or

3.9.2 has caused direct or indirect damage to the Company or a real threat of damage or has damaged the reputation of the Company.

3.10 During the process of establishing the Customer Relationship, the Company checks the Customer's compliance with the conditions set out in the Procedure on the basis of the data, documents and confirmations provided by the Customer and checks the Customer without delay, but in any case before the Customer Agreement is deemed concluded.

3.11 If the Company identifies the basis for refusing to establish a Customer Relationship in the Customer Environment when servicing the Customer, the person will be shown a corresponding error message in the Customer Environment and will not be allowed to continue the Customer Relationship creation process and enter into the Customer Agreement.

3.12 The Customer Relationship shall be deemed established and the Customer Agreement shall be deemed concluded between the Company and the Customer and binding on the parties from the moment all the following conditions are met:

3.12.1 A personal User Account has been created for the Client;

3.12.2 When using the client and the representative, the identity of the representative and the right of representation have been established in accordance with the requirements;

3.12.3 the Client has agreed to the terms and conditions of the Client Agreement and the conclusion of the Client Agreement;

3.12.4 the Client has submitted to the Company all data and documents required in accordance with the Internal Rules and legislation;

3.12.5 the Customer's User Account is personalized in accordance with the requirements;

3.12.6 there are no grounds for refusing to establish a Customer Relationship;

3.12.7 The Company has confirmed the conclusion of the Customer Agreement.

3.13 When establishing a Customer Relationship, the Company collects at least the following information about each Customer:

3.13.1 Name of the Customer;

3.13.2 Customer's personal identification code or registry code. In the absence of a personal identification code, date and place of birth;

3.13.3 Country of residence or domicile of the Client;

3.13.4 Customer's contact address;

3.13.5 Customer's telephone number;

3.13.6 Customer's e-mail address;

3.13.7 Customer's field of activity;

3.13.8 the same information about the Client's representative as about the individual Client;

3.13.9 the basis for the right of representation of the Client's representative;

3.13.10 the Client's confirmation that he / she, in the case of a legal entity, his / her Actual Beneficiary and his / her representative, is not a Person with a State Background;

3.13.11 in the case of a natural person, the Client's confirmation that he or she is the Actual Beneficiary and in the case of a legal entity, information on the ownership and control structure of the Client and the Actual Beneficiary.

3.14 When establishing a Customer Relationship, the Company shall collect at least the following documents about the Customer:

3.14.1 a copy / photograph of the identity document (facial image) used by the natural person's Client or the legal person's Client's representative in the course of identification;

3.14.2 in the case of a legal person, a printout of the registry card and / or a documentary confirmation confirming the continued operation of the legal person;

3.14.3 in the case of a legal entity, inquiries about related parties indicated by the Client;

3.14.4 if an authorized representative is used, the corresponding power of attorney. At the request of the Company, the Client with a foreign residence or his / her representative must submit a notarised or equivalent document certifying his / her authority, which is legalized or

certified with a certificate (apostille) replacing legalization, unless otherwise provided by an international agreement.

3.15 The Customer Agreement entered into between the Company and the Customer shall be made available in the Customer Environment in a form that allows the Customer to reproduce it in writing. The Company guarantees the Customer free access to the terms and conditions of the Customer Agreement at any time.

3.16 The Company retains the data and documents collected about the Customer upon establishing the Customer Relationship and the Customer Agreement entered into between the Company and the Customer in accordance with the procedure for maintaining the Company's databases and handling data and internal information and documents.

4 TERM, SUSPENSION AND TERMINATION OF THE CUSTOMER AGREEMENT

4.1 The Company enters into all Customer Agreements for an indefinite period.

4.2 Suspension of the performance of the Client Agreement shall take place under the following conditions:

4.2.1 The Company suspends the performance of the Customer Agreement if:

4.2.1.1 The Company has a suspicion that the Customer's User Account can be used or will be used by an unauthorized person;

4.2.1.2 the Client has notified the Company that his User Account can be used or will be used by an unauthorized person;

4.2.1.3 the Company has a suspicion of Money Laundering or Terrorist Financing or the Client is included in the List of Subjects of the Financial Sanction;

4.2.1.4 the Client does not submit the additional information and / or documents requested by the Company in the course of implementing the due diligence measures;

4.2.1.5 the Client has violated the terms and conditions of the Client Agreement;

4.2.1.6 there are other grounds for suspension provided for in the Client Agreement or legislation;

4.2.2 Upon the occurrence of the grounds for suspension of the performance of the Client Agreement, the Company shall immediately:

4.2.2.1 blocks the Client's User Account and notifies the Client of the suspension of the Client Agreement, its basis and blocking of the User Account, displaying a corresponding notice in the Client's environment and forwarding the notice to the Client's e-mail address, unless otherwise specified permissible in accordance with and

4.2.2.2 decides to take additional measures, including collecting additional information from the Client if necessary (for example, on the origin of funds).

4.2.3 The Company shall notify the Client of the loss of the basis for suspension of the Client Agreement, resumption of the Client Agreement and activation of the User Account or cancellation of the Client Agreement immediately after the relevant circumstances become clear, displaying a notice in the Client

4.3 The Customer Agreement terminates in one of the following cases:

4.3.1 upon the Customer's lawful withdrawal from the Customer Agreement;

4.3.2 upon the Customer's lawful termination of the Customer Agreement;

4.3.3 Upon the Company's lawful termination of the Customer Agreement.

4.4 The Customer may withdraw from the Customer Agreement under the following conditions:

4.4.1 Withdrawal from the Client Agreement is permitted within the following terms:

4.4.1.1 within 14 days as of the date of concluding the Customer Agreement; or

4.4.1.2 within 14 days as of the receipt of the pre-contractual information required in accordance with the terms and conditions of the Client Agreement and the legislation, if the information was submitted to the Client after the day of concluding the Client Agreement;

or

4.4.1.3 within three months from the date of concluding the Client Agreement, if due to a technical failure of the Company or for any other reason the Client did not provide the terms of the Client Agreement or pre-contractual information required by law, the Client is deemed to have withdrawn from the Client Agreement.

4.4.2 In order to withdraw from the Customer Agreement, the Customer shall submit to the Company through the Customer Environment or to the Company's postal or e-mail address in writing or in a form that can be reproduced in writing.

4.4.2.1 the addressee of the application, i.e. the Company;

4.4.2.2 Customer's name;

4.4.2.3 Customer's personal identification code or registry code;

4.4.2.4 a reference to the relevant Client Agreement;

4.4.2.5 an explicit statement to withdraw from the Client Agreement;

4.4.2.6 the date of preparation of the application for withdrawal from the Client Agreement;

4.4.2.7 Customer's signature.

The Management Board shall establish a standard withdrawal form in accordance with the legislation and make it available to the Clients free of charge in the Client Environment.

4.4.3 Upon receipt of the withdrawal application, the Company shall register it in the information system, notify the Customer of the receipt of the application and then decide on the term of the application and compliance with the requirements. The Company shall immediately inform the Customer of the decision made regarding his / her withdrawal application, displaying the respective notice in the Customer Environment and forwarding it to the Customer's e-mail address. If necessary, the Company shall provide the Customer with instructions for specifying a timely withdrawal application.

4.4.4 If a dispute arises with the Client regarding the legality of withdrawal from the Client Agreement, it shall be resolved, if possible, by agreement of the parties.

4.5 Regular cancellation of the Customer Agreement takes place under the following conditions:

4.5.1 The Customer has the right to cancel the Customer Agreement at any time without prior notice and without giving a reason, by deleting its User Account;

4.5.2 The Company may cancel the Customer Agreement without disclosing the reason by notifying the Customer of the cancellation of the Customer Agreement in writing or in a form that can be reproduced in writing at least two months in advance.

4.6 Extraordinary cancellation of the Customer Agreement shall take place under the following conditions:

4.6.1 both the Company and the Customer have the right to immediately cancel the Customer Agreement by submitting an application submitted in writing or in a form that can be reproduced in writing without prior notice;

4.6.2 there is a good reason if, taking into account all the circumstances and considering the interests of the parties, the party cannot reasonably be expected to continue to perform the Client Agreement. The Company may cancel the Customer Agreement in an extraordinary manner, especially if there are any grounds for refusing to establish a Customer Relationship;

4.6.3 Upon receipt of an extraordinary cancellation notice of the Customer Agreement, the Company shall immediately form an opinion thereon and notify the Customer thereof in writing or in a form that can be reproduced in writing within 14 days of receipt of the request;

4.6.4 Upon the occurrence of the grounds for extraordinary cancellation of the Customer Agreement, the Company shall immediately formulate its position thereon and, if necessary, submit to the Customer an application for extraordinary cancellation of the Customer Agreement in writing or in a form that can be reproduced in writing;

4.6.5 The Company shall try to resolve disputes related to the extraordinary termination of the Customer Agreement by agreement between the parties, if possible.

4.7 The Company shall retain all correspondence and other data and documents (especially statements of the parties) between the Company and the Customer concerning the suspension and termination of the performance of the Client Agreement in accordance with Section 9 on Maintenance of Databases and Data Processing.

5 PRESENTING THE GUIDE TO THE CUSTOMER ENVIRONMENT

5.1 In the Client Environment, the Client can submit Instructions only electronically, through the User Account.

5.2 In order to submit an Transaction, the Client must:

5.2.1 log in to the Customer Environment;

5.2.2 fill in the form in the Client Environment, which contains at least the following information about the submitted Transaction:

5.2.2.1 name of the recipient (mandatory);

5.2.2.2 Beneficiary's account number (mandatory);

5.2.2.3 the amount in the value of the instrument used (mandatory);

5.2.2.4 currency (automatically pre-filled);

5.2.2.5 Explanation or payment reference number (one of which is mandatory).

A more detailed form of the Transaction shall be established by a decision of the Management Board. The Service Fees associated with the use of the Service are automatically displayed to the Customer.

5.2.3 save the Transaction by clicking on one of the payment links selected by the Customer in the Customer Environment;

5.2.4 transfer to the bank account of the Payment Institution specified by the Company:

5.2.4.1 the amount specified in the Transactions; together

5.2.4.2 with the fee for filling in the Transaction in accordance with the Company's Price List, which is automatically displayed to the Customer when filling in the Transaction form.

5.3 The Transaction becomes binding on the Client from the moment the Transaction is duly submitted, ie the Client has completed all the steps specified in clause 5.2 of the Procedure and the amounts specified in clause 5.2.4 have been received in the Company's account.

5.4 A Client who is a legal entity may authorize a third party (eg the Client's accountant or a member of the Management Board) to submit the Transaction on its own behalf. A Client who is a natural person may not use a representative when submitting the Transaction.

5.5 The Information System shall immediately forward the Transactions to the Company for automatic execution.

5.6 The Client cannot withdraw the Order if it is deemed to have been received by the Company.

6 RECEIPT, ACCEPTANCE AND COMPLETION OF THE TRANSACTIONS

6.1 The Company accepts, accepts and executes the Transactions submitted by the Clients:

6.1.1 every day, including weekends, public holidays, etc.;

6.1.2 at any time;

6.1.3 only if the assets necessary for the execution of the Transaction are received by the Company by transfer, i.e. the Service is not settled in cash.

6.2 The Transaction shall be deemed binding on the Company from the moment it is deemed to have been received by the Company.

6.3 The Transaction shall be deemed to have been received by the Company if:

6.3.1 The Client has submitted the Transactions; and

6.3.2 The amount required to execute the Transaction has been received in the Company's account; and

6.3.3 there are no grounds for refusing to accept and comply with the Transactions.

6.4 Upon receipt of the Transaction, the Company shall immediately check whether all the preconditions for the acceptance and fulfillment of the Transaction have been met in accordance with the requirements. The check is usually performed automatically. If for any reason an automatic check is not possible, the check is performed manually.

6.5 Acceptance and compliance with the Transactions presupposes that:

6.5.1 a Client Account has been created for the Client and it has been duly personalized;

6.5.2 the Customer Agreement entered into with the Customer is valid, its performance has not been suspended and there are no grounds for suspending the performance of the Customer Agreement or canceling the Customer Agreement;

6.5.3 the identity and right of representation of the Client and his / her representative have been duly established;

6.5.4 the Client has submitted to the Company all documents and data required by law, including for the prevention of money laundering and terrorist financing and for compliance with the requirements of international financial sanctions;

6.5.5 the Client has submitted a Transactions that meet the requirements;

6.5.6 The Company has received the values required to fulfill the Transaction;

6.5.7 The current account of the Beneficiary Customer is a current account opened with a credit institution registered in a Contracting State of the European Economic Area or a branch of a third country credit institution registered in the European Economic Area or a credit institution or financial institution in a third country subject to Directive (EU) 2015/849 requirements and the fulfillment of which is subject to state supervision

6.5.8 If necessary, the Transactions state the disbursement of funds through a partner who has entered into an outsourcing agreement with the Company; and

6.5.9 There are no grounds for refusing to comply with the Transactions.

6.6 The Company may not refuse to comply with the Transactions, the preconditions for acceptance and performance of which have been duly fulfilled.

6.7 If all the preconditions for acceptance and fulfillment of the Transaction have been fulfilled in accordance with the requirements, the Company shall make a decision on acceptance and fulfillment of the Transaction without delay, but no later than within the period paid down in Section 6.10.

6.8 Upon execution of the Transaction, the Company may, if necessary, transfer the activities related to the provision of the service to a third party if it is necessary for the execution of the Transaction given by the Customer.

6.9 If there are preconditions for acceptance and fulfillment of the Transaction, the Company shall make a decision to refuse to accept and comply with the Transaction only if:

6.9.1 The Company does not consider it possible to implement the measures specified in clause 4.2 of the Procedure; or

6.9.2 The implementation of the measures specified in clause 4.2 of the Procedure has not been effective.

6.10 If one or more of the preconditions for the acceptance and fulfillment of the Transaction submitted in the Client's environment are not duly fulfilled, the Company shall, if possible, take one of the following measures:

6.10.1 if the Customer has submitted a non-compliant Order (for example, the name of the payee and the payee's bank account number do not match), the Company shall notify the Customer immediately, but not later than within 24 hours If the Client does not eliminate the deficiencies within 24 hours as of the display of the respective notice to the Client, the Company shall immediately make a decision not to accept and comply with the Transactions and inform the Client thereof by displaying the respective notice in the Client environment;

6.10.2 if the Customer fails to transfer the funds necessary for the execution of the Order to the Company's account within 24 hours from the recording of the Order (i.e. after the execution of the Payment Order in the Customer Environment), the Company shall notify the Customer immediately, but not later than within 24 hours, displaying the corresponding message to the Customer in the Customer Environment. If the Client does not transfer the amount necessary for the execution of the Order to the Company's account within 24 hours from the display of the notice, the Company shall immediately decide not to accept the Order and execute it and inform the Client thereof by displaying the corresponding notice in the Client environment;

6.11 In the event of non-acceptance and non-execution of the Order, the Company shall in any case return the funds transferred for the execution of the Order to the Client without delay, taking into account the time reasonably necessary to make the refund. The Company shall deduct from the funds returned to the Customer the direct costs and service fee associated with the return thereof in accordance with the Company's Price List.

7 PROVIDING INFORMATION TO THE CUSTOMER ON COMPLETION OF THE TRANSACTIONS

7.1 Prior to the execution of the Transaction, the Company shall, at the request of the Client, provide the Client with information on the term for the execution of the Transaction, the fees payable, the bases for their formation or distribution.

7.2 After completing the Transactions, the Company shall immediately provide the Customer with the following information:

7.2.1 the number or other identifier of the Transaction that enables the Transaction to be identified;

7.2.2 Recipient of the Transaction;

7.2.3 the amount of funds transferred on the basis of the Transactions in the currency indicated in the Transactions;

7.2.4 the amount of fees payable for the execution of the Transaction;

7.2.5 Date of receipt of the Transaction.

8 DEADLINE FOR COMPLIANCE WITH THE GUIDE PROVIDED IN THE CUSTOMER ENVIRONMENT

8.1 The Company shall execute the received and compliant Transactions within the term specified in the Customer Agreement in the Customer Environment, but in any case in such a way that the payment amount indicated in the Transactions is credited to the payee's payment service provider's account no later than on the settlement day.

9 PROCEDURES FOR NON-COMPLETED OR INCORRECTLY COMPLETED TRANSACTIONS

9.1 In case of non-executed or incorrectly executed Transactions, the Client has the right to demand from the Company:

9.1.1 Immediate and non-deductible refund of funds transferred to the Company's account for the execution of the Transaction; and

9.1.2 Refund of fees transferred to the Company's account for the execution of the Transaction.

9.2 The Client has no right to cancel the Transactions after the Transactions have been read.

9.3 The Company shall make a decision regarding the Customer's claim no later than within 14 days as of the receipt of the respective claim. If the Customer's claim is justified, the Company shall execute the claim without delay, unless the Company proves that the funds specified in the Transactions were received on time and without deduction to the payee's payment service provider's account no later than on the settlement day following receipt of the Transactions.

9.4 If the Company has not complied with the Transactions or has complied with them incorrectly, the Company shall, at the Customer's request, notwithstanding its liability, determine the material circumstances related to the transaction and inform the Customer within a reasonable time but not later than 15 working days after receiving the complaint. The notice will be sent to the Customer's postal address or e-mail address, unless otherwise agreed with the Customer.

9.5 If the Company fails to respond to the Customer's request or take all necessary actions to resolve the request for reasons beyond its control, the Company is obliged to justify the reason for the delay to the Customer and set a deadline for completion of the necessary actions, which may not exceed 35 business days.

9.6 Upon ascertaining the circumstances of the Customer's claim, the Company shall assess the existence of a possible operational or security incident related to the service provided.

9.7 The Management Board shall register the incident in a file of the register of operational and security risks approved by the Management Board of the Company, which shall be submitted to the state institutions in accordance with applicable laws and other legislation.

10 TRANSFER OF RESOURCES TO BE TRANSFERRED AND REMUNERATION OF FEES AND OTHER EXPENSES

10.1 The Company is obliged to transfer the funds indicated in the Transactions and transferred by the Client to the Company's account on the basis of the Transactions in full to the recipient specified in the Transactions. The Company will not deduct any fees, expenses, etc. from this amount.

10.2 The Client is obliged to transfer the service fee and other fees necessary for the execution of the Transaction in accordance with the Price List to the Company's account. Payment of these amounts to the Company's account is one of the preconditions for acceptance and execution of the Transaction.

11 PLAN TO DETERMINE, REDUCE OR PREVENT THE RISK OF BUSINESS INTERRUPTION

11.1 The risks of business interruption shall be determined in accordance with the Internal Rules "12. Procedures for Risk Management and Business Continuity". The most significant risks of business interruption are primarily related to failures of information systems, as the Company's operations are largely based on information technology solutions.

11.2 Various measures shall be taken to mitigate and prevent the risk of business interruption of the Company in accordance with the internal rules of procedure provided for in the Internal Rules, in particular in accordance with the Procedure "8. Procedure for Security and Control of Information Technology Systems", and Section 9: Procedures for the maintenance of databases, processing of data and movement of internal information and documents.

11.3 In the event of a business interruption, the Management Board is responsible for resuming operations.

4. EXECUTION OF TRANSACTIONS

1 PURPOSE

1.1 The purpose of the procedure is to determine:

- Procedure for performing transactions and operations of the Company;

- Principles of investing the company's assets;

- Compliance with the requirements of the Procedure and proper compliance of the Procedure by the Managers and Employees

- the persons responsible for inspection.

2 RESPONSIBILITY

2.1 The Management Board 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 STORAGE PRINCIPLES

3.1 The Company shall keep the Client's funds transferred to it from the provision of the Services separate from its own assets and from the assets not related to the provision of the Services.

3.2 The Client's funds entrusted to the Company in connection with the provision of services belong to the Client related to the provision of the service, it is not included in the Company's bankruptcy assets and the claims of other creditors of the Company are not satisfied.

3.3 Funds entrusted to the Company in connection with the provision of services are not insured.

3.4 The Company shall open separate accounts in its own name for credit institutions registered in the Contracting State of the European Economic Area of its choice for servicing the Transactions initiated in the Client Environment, in which the Company may perform only the following transactions:

3.4.1 Receipt of funds transferred by customers;

3.4.2 Return of funds transferred to customers by them;

3.4.3 Transfers required to balance the liquidity reserves of separate accounts opened for the Company to provide the Service to the Clients;

3.4.4 other transactions related to the provision of the Service, including the transfer of the service fees paid by the Clients to the Company to the Company's own funds account.

3.5 The Management Board sets limits for the accounts specified in clause 4.4 of this Procedure and maintains them at a reasonable level, taking into account the Company's needs and level of risk. The Company shall ensure that only persons authorized to comply with the Transactions have access to the Company's accounts specified in clause 4.4.

3.6 The Company shall perform transactions with the Customer's funds only in accordance with the Customer's Payment Transactions and / or the Customer Agreement and / or legislation. Other transactions with the Client's funds are prohibited, including the investment or storage of the Client's funds. If the Client transfers funds to the Company's account but does not submit the Transactions corresponding to the funds (on time), the Company shall return the funds to the Client in accordance with the Company's Service Provision Procedure.

3.7 The Company shall keep separate records of the Transactions submitted by the Customer, the funds transferred by the Customer to the Company and the Transactions submitted by the Customer and executed or not executed by the Company, so that transactions and operations performed by the Company with the Customer's funds.

3.8 The Company collects and stores data on transactions made with the Company's and the Clients' funds in such a way that the Company can at any time without delay distinguish each Client's funds from other Clients' funds and the Clients' funds from the Company's own funds.

4 TRANSACTION IN THE NAME AND ACCOUNT OF THE COMPANY

4.1 The Company enters into transactions and operations in its own name and on its own account in accordance with legislation and the decisions of the Company's Articles of Association and management bodies.

4.2 The Company shall use special separate accounts for this purpose in its own name and for its own account.

4.3 All transactions and operations performed by the Company in its own name and on its own account shall be documented in accordance with the Company's internal accounting rules.

5 INVESTMENT OF COMPANY RESOURCES

5.1 The company uses its resources primarily to carry out its day-to-day business.

5.2 The Management Board decides on the investment of the Company's available funds.

5.3 The Company invests free funds primarily in the development and improvement of the services provided by the Company and the information systems necessary for their provision, in the marketing of the provided services and, if possible, in the expansion of the Company's economic activities.

5.4 The Company does not invest its assets in bonds or similar instruments.

5.5 The Company does not grant loans, except for intra-group loans, the detailed terms of which are decided by the Management Board when the need arises.

5.6 The Company may deposit its funds only in deposits offered by credit institutions and keep them in the Company's current accounts only on such terms that the Company's liquidity is guaranteed at all times and the Company can use the funds without significant delay, i.e. terminate the deposit agreement, etc.

5. OUTSOURCING PROCEDURE

1 PURPOSE

1.1 The purpose of the procedure is to determine:

- Extent of outsourcing of the company's activities;

- Prerequisites for outsourcing of the company's activities;

- Procedure for deciding on outsourcing of the company's activities;

- Terms of the agency agreement;

- The person responsible for the proper execution of the activities outsourced by the company;

- Procedure for notifying the company of the transfer of activities;

- Compliance with the requirements of the Procedure and proper compliance of the Procedure by the Managers and Employees

2 RESPONSIBILITY

2.1 The Management Board is responsible for the compliance of the procedure with the requirements and its proper compliance.

2.2 The Risk Manager is responsible for checking the compliance of the procedure with the requirements and its proper compliance.

2.3 The procedure is obligatory to comply primarily with the Managers, but also with all Employees, whose competence includes deciding on the transfer of the Company's activities to the extent determined by the Management Board.

3 DEFINITION AND SCOPE OF OUTSOURCING

3.1 Outsourcing of the activities of the Company is the transfer of the activities and operations related to the provision of the Service to a Third Party (i.e. the Service Provider) on the basis of the Agreement, taking into account the special requirements and restrictions provided by legislation and the Procedure.

4 CONDITIONS FOR OUTSOURCING OF ACTIVITIES

4.1 The Company has the right to outsource the activities related to the provision of the Service to a Third Party if all the following conditions are met:

4.1.1 the outsourcing of activities enables the Company to better fulfill its obligations;

4.1.2 Managers do not delegate their responsibilities by delegating activities;

4.1.3 the outsourcing of activities does not harm the Clients' interests or relations with the Clients;

4.1.4 the outsourcing of activities does not change the Company's obligations to the Clients;

4.1.5 the outsourcing of the activity is not in conflict with the conditions provided by legislation, which the Company must meet in order to obtain or remain in compliance with the activity license;

4.1.6 when outsourcing activities directly related to customer service to the service provider, an activity license of the competent authority is required;

4.1.7 the outsourcing of activities does not hinder the activities of the Company and the fulfillment of its obligations by the Company to the required level;

4.1.8 the person to whom the activities are delegated has an impeccable reputation, the necessary knowledge and skills for the reliable and professional performance of the duties and is able to perform the duties delegated to him;

4.1.9 the transfer of the activity does not revoke or change the conditions on the basis of which the Company was granted an activity license;

4.1.10 in case of outsourcing of activities within the group, all requirements apply;

4.1.11 the transfer of activities does not prevent the proper performance of the Company's internal control or the exercise of the necessary level of supervision over the Company;

4.1.12 other legal requirements have been met.

5 OUTSOURCING RISK ASSESSMENT

5.1. Before deciding on the outsourcing of activities, a corresponding risk assessment is prepared and approved by the Management Board of the Company. The outsourcing risk assessment shall analyze at least the following:

- the impact of the outsourcing on the Company's business and the risks involved;

- the reporting and monitoring procedures applied to the transfer of activities (incl. description of the transfer of activities, conclusion of the contract, performance of the contract until its expiry, strategies for termination of the contract);

- in the case of outsourcing, the selection of the person who will supervise the service provider, the evaluation procedure and the methodology.

5.2. In addition, where the outsourcing involves a significant function, the potential impact of not performing the outsourced function should be assessed:
- short-term and long-term Company's (financial) capacity;
- business continuity;
- operational risk;
- reputational risk;
- customer services;
- the possible impact on the Company and Customers of the violation of data protection and confidentiality requirements or the lack of data availability or integrity.

6 DECISION ON THE TRANSFER OF ACTIVITIES

6.1 The transfer of the Company's activities shall be decided by the Management Board, which shall assess:

6.1.1 whether the outsourcing is necessary and how it will improve the provision of the service;

6.1.2 whether the preconditions set out in clause 5 of the Procedure have been met;

6.1.3 what are the costs, savings or revenues associated with the transfer of the activity;

6.1.4 whether the Third Party to whom the activity is outsourced is competent and fit for the outsourced activity, to the extent necessary for the background examination necessary to make such an assessment;

6.1.5 what measures are taken to ensure that the Third Party to whom the activity is outsourced complies with all legal acts regulating the activity, etc. in the implementation of the adopted activity;

6.1.6 how the risks associated with the outsourcing of activities are managed;

6.1.7 how supervision is exercised over the Third Party to whom the activity is outsourced.

6.2 The Company's obligation to identify in part or in full the identity, beneficial owner, identification of the person with a State Background, source and / or origin of wealth and the purpose and nature of the business relationship / transaction is provided only by:

- to another obligated person;

- an organization, association or union of which persons within the meaning of AML/CTF Law are required to be members, or;

- to any other person who applies the due diligence and data retention requirements set out in the Money Laundering Act and the Internal Rules and who is or is prepared to be subject to anti-money laundering or financial supervision in a Contracting State of the European Economic Area.

6.3 The obligation to apply due diligence measures within the meaning of AML/CTF Law not mentioned in clause 7.2 shall not be transferred. This restriction does not apply to the transfer of activities related to the identification and implementation of an international sanction.

6.4 The activity shall not be granted to a person established in a high-risk third country.

7 TERMS AND CONDITIONS OF THE TRANSFER AGREEMENT

7.1 In order to transfer the activities, the Company enters into an agreement with the Third Party, which defines the nature and scope of the transferred activities and the rights, obligations and responsibilities of the parties in such a way that they are unambiguous, enforceable and controllable.

7.2 The contract governing the transfer of activities must specify, inter alia, where applicable:

7.2.1 the distribution of the rights and obligations of the parties and their content;

7.2.2 requirements for outsourced activities;

7.2.3 Remuneration and other benefits payable to a third party;

7.2.4 liability of the parties and legal remedies;

7.2.5 the Company's right to receive information from the Third Party about the outsourced activities;

7.2.6 the right of the Company to give the Third Party the Transactions necessary for the performance of the activities;

7.2.7 information technology security issues (if applicable);

7.2.8 obligation of confidentiality (if applicable);

7.2.9 Guarantees and warranties provided by a third party (if applicable);

7.2.10 Permissibility of additional outsourcing of activities transferred by a Third Party;

7.2.11 the bases, conditions and procedure for amending, terminating and terminating the contract;

7.2.12 choice of applicable law (which must not prevent adequate supervision).

8 OUTSOURCING SUPERVISION AND RESPONSIBILITY

8.1 The company must exercise due skill, care and diligence in the outsourcing of important activities related to the provision of the service, including the conclusion, performance and termination of contracts.

8.2 Upon outsourcing of activities related to the provision of the service, the Management Board shall be responsible for supervising the respective service provider, involving Employees with the necessary skills.

8.3 If there have been significant changes in the outsourced activity or in the service provider (eg in the service provider's financial position, ownership), a new assessment must be made of the service provider. In the case of an outsourced essential function, this assessment must be performed at least once a year.

8.4 Upon outsourcing of activities, the Company is responsible for the proper performance of the activities.

6. 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 fulfillment of the requirements arising from the AML/CTF Law and includes the rules of procedure for the proper fulfillment 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 Lithuania, 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 fulfill 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 Republic of Lithuania “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 behavior;

- 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 fulfillment 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 Lithuania 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 Lithuania;

4.6.3 a government agency of Lithuania 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 an Lithuanian 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 Lithuania; 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 Republic of Lithuania 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 Republic of Lithuania. 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 Republic of Lithuania 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 Republic of Lithuania.

11 IDENTIFICATION OF LEGAL ENTITIES

11.1 The company shall identify the identity of a legal person registered in the Republic of Lithuania 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 Republic of Lithuania 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 apostilized. 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 analyze 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 (ies) 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, ie 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 analyze 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 Adverese 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 fulfillment 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 analyzing 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 Fulfillment of other obligations related to the fulfillment 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 (ie 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 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 analyze the risks related to its activities. The steps taken to identify, assess and analyze 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 Republic of Lithuania;

- 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 Republic of Lithuania is identified while staying in the same place

- a client who is a legal person entered in the commercial register of the Republic of Lithuania, 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.

7. 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 behavior 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 analyzed).

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

Afganistan	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	Macaco 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

7. 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 analyze 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, analyze 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 behavior 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 analyzes 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 is 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 Defense, where:

7.5.1 The First Line of Defense, ie the business area, is responsible for risk-taking and day-to-day management;

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

7.5.3 The Third Line of Defense, ie 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.

8. SECURITY AND INFORMATION SYSTEMS OF INFORMATION TECHNOLOGY SYSTEMS INSPECTION PROCEDURES

1 PURPOSE

1.1 The purpose of the procedure is:

- give an overview of the important parts of the Company's IT system;

- determine the security requirements of the Company's IT system;

- determine the Company's organizational security requirements;

- determine the security control requirements for the Company's IT systems;

- determine the persons responsible for checking the compliance of the Procedure with the requirements and the proper compliance of the resulting instructions with the Employees.

2 RESPONSIBILITY

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

2.2 The Management Board may transfer the respective activities to the Employees or to third parties in accordance with the Procedure for Transfer of Activities

2.3 The procedure is mandatory for all Managers and Employees.

3 INFORMATION SYSTEM COMPONENTS

4.1 The company's information system consists of the following parts:

4.1.1 Company's public website and mobile application;

4.1.2 Customer Environment integrated into the Company's website with limited access;

4.1.3 Company intranet;

4.1.4 The company's core system.

4.2 The relationship between the Company and the Client takes place through the Client environment, incl.

4.2.1 Creating and personalizing a user account;

4.2.2 Identification of the Client and his / her representative (except to the extent that this is done while in the same place);

4.2.3 Entering into a Customer Agreement;

4.2.4 Submission of instructions;

4.2.5 Displaying information (incl. Error messages) on the execution of instructions to the Clients;

4.2.6 Submission of claims by the Clients to the Company;

4.2.7 The Company's response to Customer's claims, etc., etc.

4.3 The following takes place via the Intranet:

4.3.1 Management of customer accounts, including blocking them if necessary;

4.3.2 Completion of the Instructions submitted by the Clients;

4.3.3 Gathering information on the receipt of funds required to fulfill the instructions;

4.3.4 Reporting and elimination of errors that have occurred during the execution of the instruction and publishing information thereon (incl. Making the relevant information available to the Client);

4.3.5 collecting and storing information necessary for reporting (incl. On the volumes of the provided Service, fees, etc.) and preparing reports on the basis thereof.

4.4 Core system:

4.4.1 provides input to the Company's website, mobile application, Customer Environment and intranet;

4.4.2 automatically checks the receipt of the funds necessary for the execution of the Instructions, after which it sends the corresponding notifications to the intranet;

4 INFORMATION SYSTEM SECURITY REQUIREMENTS

5.1 The Company uses only SSL-certified and firewall-protected Internet connections.

5.2 In order to prevent denial-of-service attacks against the Company's website and mobile application, the Company uses only RESTful APIs for connection interfaces.

5.3 As a rule, the different parts of the information system are placed on separate servers. If parts of the information system reside on a single server, they shall be clearly separated within that server by access that is subject to different access restrictions and firewall settings.

5.4 The customer passwords of the Customer's Customer Environment are stored in encrypted form.

5.5 The Company keeps a log of all transactions and operations performed on behalf of the Company as well as the Clients. The log is saved and maintained in a playable format.

5.6 The enterprise system provides system administrators with automatic notification of critical system errors, problems, and abnormalities.

5.7 The public services provided by the company are protected against DDOS attacks.

5.8 The Company's system backs up the Company's electronic databases at least once a day. To ensure fault tolerance, the Company's master-slaves are duplicated and run on RAID1 or RAID5 disks.

5.9 The Management Board or a person appointed by the latter shall check at least once a week for security updates for the Company's server operating system and the software used on the servers. If security software updates are available, updates will be installed as needed.

6 ORGANIZATIONAL SECURITY REQUIREMENTS

6.1 In order to secure the computers of its employees, the Company applies the following security measures:

6.1.1 computer hard drives must be encrypted;

6.1.2 When away from the computer, the computer must be locked (so-called screen saver mode) and then the computer must be accessible only with a username and password. If the computer is not in use, the computer must lock itself within a reasonable time;

6.1.3 the computers have a working firewall and anti-virus;

6.1.4 mobile telephones must be protected by a key lock;

6.1.5 Security updates for computers and mobile phones are installed at least once a week.

6.2 The Company shall provide the Managers, Employees and the Partner with access only to the information necessary for the performance of their duties. Access shall be granted in accordance with the procedures for the maintenance and handling of databases and the flow of internal information and documents.

6.3 The company shall document the design of the system and the parameters used.

6.4 Server passwords are stored securely. Access to server passwords is restricted to system administrators and, in an emergency, to Managers.

7 SECURITY CONTROLS AND FOLLOW-UP OF INFORMATION SYSTEMS

7.1 During the security audit of the company's IT systems, the following shall be checked:

7.1.1 compliance of the IT software and infrastructure with the requirements set out in these Procedures; and

7.1.2 the operation of the security components of the systems (in particular firewalls).

7.2 The security and operational control of the IT system is performed in three different ways:

7.2.1 manual inspection before and after upgrades or more than 3 months after the last inspection. As part of the inspection, the responsible person checks whether the system complies with the requirements, including security requirements;

7.2.2 automatic interval control, i.e. a server-side log tracking system that alerts the responsible person at least once a day to errors or suspicious queries;

7.2.3 real-time automatic monitoring, i.e. an automatic mechanism integrated into the system that notifies the responsible person in real time of errors and problems in the system.

7.3 In addition to performing internal security and performance control of the IT system, the Company also uses an independent IT solution testing service.

7.4 The Company shall conduct a quarterly audit of the implementation of IT system security measures, during which compliance with the IT system security requirements reflected in these Procedures shall be verified and a risk assessment shall be performed, on the basis of which these Procedures shall be amended and / or supplemented.

7.5 The Company will check once a month for the existence of backup copies of the Company's electronic databases and test the system recovery from backups.

7.6 The responsible person shall report the results of the IT systems audit to the CEO of the Company, who shall examine the report prepared by the responsible person and confirm the review of the report with a signature.

7.7 If the responsible person identified deficiencies during the inspection of the IT systems, the Management Board shall appoint a person who shall prepare an action plan for the elimination of deficiencies and be responsible for the implementation of the respective action plan.

9. MAINTENANCE OF DATABASES, DATA PROCESSING AND INTERNAL INFORMATION AND PROCEDURE FOR THE MOVEMENT OF DOCUMENTS

1 PURPOSE

1.1 The purpose of the procedure is to determine:

Databases maintained by the company;

- The persons responsible for the processing of the company's databases, the persons authorized to process the databases and the procedure for granting authorization to process the database,
- Tasks of the chief processor and authorized processor of the company's database;
- The manner and terms of maintaining the company's databases;
- Procedure for the transmission of internal information;
- Persons responsible 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 Management Board 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 DATABASES

3.1 The company maintains the following databases, which contain:

3.1.1 Information and documents concerning the management of the company, employees and supervision:

- management documents, including the Company's founding documents, articles of association, decisions of management bodies and minutes of meetings, credentials, directives, etc .;

- Budgets and other strategic documents concerning the company;

- Documents concerning Managers and Employees, including employment and service contracts and amendments thereto, job descriptions, termination documents, etc .;

- agreements concluded for the outsourcing of services and transfer of the Company's activities, related correspondence and reports;

- Valid and invalid versions of the Internal Rules;

- internal control plans, plans, reports and related documents;

- documents relating to the exercise of supervision, including inquiries, precepts from the supervisory authorities and the answers given to them;

- documents, notices, etc. concerning the prevention of money laundering and terrorist financing and the application of financial sanctions;

- register of customer complaints;

- register of breaches of sensitive payment data.

3.1.2 Data and documents concerning the provision of the Service to the Customer:

- Customer's personal data;

- Additional data and documents submitted by the Customer upon identification and collected in connection therewith;

- Instructions submitted by the Client;

- Customer Agreements concluded with the Customer;

- Documents related to the performance of the Client Agreement and related correspondence;

- Applications for withdrawal from the Customer Agreement and cancellation of the Customer Agreement and related correspondence;

- Customer complaints, claims and claims and the answers given to them;

- Inquiries and other communications sent to the Customer and the answers given to them;

3.1.3 accounting and reporting data and documents:

- basic accounting documents, including purchase and sales invoices, etc .;

- documents concerning the calculation of remuneration;

- bank documents;

- tax returns;

- one-off, quarterly and annual reports and their annexes;

- audit reports and their annexes;

3.1.4 data and documents concerning the Company's information systems:

- architecture, including security;

- regular and extraordinary maintenance;

- error messages;

- innovations;

- service;

- inspection and audit;

3.1.5 Other mandatory information and documents required by law.

4 RESPONSIBLE AND AUTHORIZED PROCESSORS OF DATABASES

4.1 The following persons are responsible for the processing of databases:

4.1.1 The CEO of the Company is responsible for the database referred to in clause 4.1.1 of the Procedure;

4.1.2 The Management Board is responsible for the database referred to in clause 4.1.2 of the Procedure;

4.1.3 The Management Board and the Accountant are responsible for the database referred to in clause 4.1.3 of the Procedure;

4.1.4 The Management Board is responsible for the database referred to in clause 4.1.4 of the Procedure;

4.1.5 The Management Board is responsible for the database referred to in clause 4.1.5 of the Procedure.

4.2 Authorization, suspension, termination and restoration of the processing of the database:

4.2.1 if the employee's right to process the database is not prescribed by clause 5.1 of this Procedure, the person responsible for processing the database shall decide to grant the Employee the corresponding authorization. The person responsible for processing the database may grant authorization on his or her own initiative or on the basis of a request submitted by another Employee. If the database is maintained electronically, the person responsible for processing it shall draw up instructions for granting the authorization in order to ensure that the authorized person has access to the electronic database specified in the authorization;

4.2.2 the person responsible for processing the respective database shall decide on the suspension, revocation and restoration of the authorization granted for the processing of the database. If the database is electronic, the person responsible for processing the database shall, upon suspension, revocation or restoration of the authorization, without delay transmit a corresponding instruction on the basis of which the person with the corresponding rights terminates or restores the access necessary for processing the database.

4.3 Transfer of Data and Documents Included in the Database to a Third Party:

4.3.1 all databases maintained by the Company are of a confidential nature and must be protected from Third Parties and the public;

4.3.2 data and documents belonging to the database may be transferred to a Third Party only with the prior written consent of the person responsible for processing the database, who may consent to their transfer only if it is required by law or permitted by the Internal Rules.

5 DUTIES OF THE RESPONSIBLE AND AUTHORIZED PROCESSOR OF THE DATABASE

5.1 The person responsible for the processing of the database is required to ensure that the database is maintained and that the data contained therein are processed in accordance with the requirements, whereby:

5.1.1 the maintenance of a database shall include the processing of the data contained therein, the keeping of records of the processing of data, the protection of data and the organization of such activities;

5.1.2 The collection, storage, organization, storage, modification, retrieval, extraction, use, transfer, aggregation, closure, deletion and destruction of data shall be considered as processing of the database.

5.2 The authorized processor of the database is required to perform all the tasks assigned to him or her by the chief processor of the database in maintaining and processing the data, including the authorized processor of the database:

5.2.1 enter the data necessary for the registration of data and documents into the database, if such database requiring registration has been created by the Company (incl. Title, date and number of the document, name of the compiler, location and term of storage);

5.2.2 saves the electronically submitted document in the correct electronic database;

5.2.3 if the document submitted on paper must be stored in an electronic database, make an electronic copy of the document submitted on paper, store it in the correct electronic database and archive the document submitted on paper in the archives;

5.2.4 processes data and documents under appropriate conditions and ensures their usability, authenticity and preservation in accordance with the requirements provided in the Internal Rules and legislation;

5.2.5 upon receipt of an instruction from the chief processor, the database shall destroy the data or documents contained therein, provided that the term for their storage has expired.

6 METHOD AND DURATION OF STORAGE OF DATABASES

6.1 As a general rule, all databases are stored electronically.

6.2 The originals of the documents submitted on paper shall be kept in the relevant archives. If necessary, a copy of the original document submitted on paper shall be made in the electronic database.

6.3 The data and documents listed in clause 4.1.1 of the Procedure shall be stored in accordance with the following:

6.3.1 Documents concerning the Managers and the Employees for at least 10 years after the termination of the employment or service contract, unless the Manager or the Employee intentionally breached the contract, in which case the data and documents shall be kept for at least 13 years after the termination of the employment or service contract;

6.3.2 other information and documents listed in clause 4.1.1 of the Procedure within the term prescribed by law after the dissolution of the Company.

6.4 The data and documents listed in clause 4.1.2 of the Procedure shall be retained for at least 5 years after the termination of the Agreement, unless the Customer intentionally violated the Agreement, in which case the Company shall retain the data and documents for at least 10 years.

6.5 The data and documents listed in clause 4.1.3 of the Procedure shall be stored in accordance with the following:

6.5.1 source accounting documents for 7 years from the end of the financial year in which the respective source document was recorded in the accounting;

6.5.2 accounting records, contracts, reports and other commercial documents necessary for a clear description of the economic transactions during the audit, 7 years from the end of the respective financial year;

6.5.3 commercial documents related to long-term obligations or rights 7 years after their expiry;

6.5.4 7 years after the amendment or replacement of the internal accounting rules;

6.5.5 The documents used as the source of the original data used to compile the report submitted for monitoring purposes for at least 5 years.

6.6 The data and documents listed in clause 4.1.4 of the Procedure shall be kept for at least 5 years.

6.7 The data and documents listed in clause 4.1.5 of the Procedure shall be preserved in accordance with the terms established in the relevant legislation.

7 PROCEDURE FOR INTERNAL TRANSMISSION OF INFORMATION AND DOCUMENTS

7.1 Information provided internally must be relevant, true, accurate, complete, clear, valid and timely, and comply with legal and internal requirements.

7.2 The information transmitted internally shall be transmitted as follows:

7.2.1 the information and documents to be stored in the electronic database shall be transmitted via the respective electronic database. If necessary, the data recorder shall also inform the recipient of the information of the storage of the information by other means of communication (verbal, telephone, Skype, e-mail, etc.);

7.2.2 information and documents that do not need to be stored in the electronic database shall be transmitted by any other appropriate means.

7.3 The information or document shall be provided immediately to the person authorized to use it or his substitute or, if the authorized person or his substitute cannot be identified, to the person who normally uses such information or document in the course of his duties or to his substitute.

7.4 If an information or document reaches a person who is not authorized to use it, the latter shall immediately forward it to the person authorized to use the information or document or his substitute, or to the person who normally authorizes such information or document in the course of his duties. uses or his substitute.

7.5 If a form enabling reproduction in writing is not required for the formalization of a work order in accordance with the Internal Rules or applicable legislation, the person transmitting the order shall take into account the nature of the work order and the term for execution.

7.6 Only the contact details of the Managers or Employees related to the Company's domain or other information notified by the Management Board shall be used for the transmission of information or documents. The Management Board is responsible for the correctness of the contact details of the Managers and the person to whom the Employee is responsible is responsible for the correctness of the contact details of the Employee.

7.7 Meetings shall be held as necessary to provide internal information and guidance to Managers and Employees. All persons invited to attend the meeting are required to attend. A meeting may be refused only if the absence is objectively justified by the volume of work, leave or sick leave, or if the absence has been authorized by the person accountable.

7.8 Meetings of the Company's management bodies (ie the shareholders, the Management Board and (if any) the Supervisory Board) are held in accordance with the legislation and the Company's Articles of Association.

7.9 All meetings of the Company's management bodies and, if necessary, also information meetings shall be recorded. The minutes shall be prepared by the chairman of the meeting or a person appointed by him and shall be stored by type (general meeting of shareholders, meeting of the management board, information meeting, etc.) in the prescribed database.

10. DUTIES, SUBSIDIARIES, REPORTING AND DUTIES OF MANAGERS AND STAFF PROCEDURE FOR DELEGATION

1 PURPOSE

1.1 The purpose of the procedure is to determine:

- Duties and responsibilities of managers and employees;
- Subordinate relations between managers and employees;
- Management and Employee Reporting Chains and Reporting Procedures;
- Procedure for Delegation of Duties and Responsibilities of Managers and Employees;
- The person responsible for checking the compliance of the procedure with the requirements and the compliance of the resulting instructions with the requirements of the Employees.

2 RESPONSIBILITY

2.1 The person to whom the respective Manager or Employee is accountable is responsible for checking the compliance and proper compliance with the requirements of the procedure (the relevant part).

2.2 The procedure is mandatory for all Managers and Employees.

3 DUTIES AND RESPONSIBILITIES OF MANAGERS AND EMPLOYEES

3.1 The tasks of the customer service representative (specialist) are:

3.1.1 Introducing the Services to the Client and providing related explanations;

3.1.2 Providing the Client with the necessary explanations for creating a User Account;

3.1.3 deciding on establishing a Customer Relationship with the Customer and concluding a Customer Agreement;

3.1.4 Identification of the Client and related advice to the Client;

3.1.5 providing the Client with explanations regarding the terms and conditions of the Client Agreement and its conclusion;

3.1.6 Providing the Client with the explanations necessary for submitting the Instruction;

3.1.7 deciding on the acceptance of the Client's Instructions, including checking the receipt of funds necessary for the execution of the Instructions;

3.1.8 Execution of the Client's Instruction;

3.1.9 Storing information related to the instruction in the Company's databases;

3.1.10 communication with the Client in connection with the performance of the Client Agreement (incl. Breach);

3.1.11 processing of complaints submitted by the Customer and making initial decisions regarding them;

3.1.12 Informing the contact person of suspicion of Money Laundering or Terrorist Financing;

3.1.13 Storing customer relationship information in appropriate databases.

3.2 The duties of the CEO are:

3.2.1 General management of the company;

3.2.2 Arranging and conducting the company's internal control;

3.2.3 Ensuring the prevention of money laundering and terrorist financing and the application of financial sanctions;

3.2.4 Organizing the daily economic activities of the Company in accordance with the principles of protection and preservation of the Client's assets, the Investment Policy;

3.2.5 Organizing the maintenance of the company's databases and data processing in accordance with the procedure for maintaining databases, data handling and the flow of internal information and documents;

3.2.6 Arranging the company's accounting, reporting and, if necessary, audit in accordance with the Accounting Procedures;

3.2.7 Arranging the liquidity of the Company's payment accounts;

3.2.8 Company marketing (in general);

3.2.9 Communicating with credit institutions, payment institutions, the Financial Intelligence Unit, the Tax Board, etc. on behalf of the Company;

3.2.10 Coordinating the establishment of the company's information systems and ensuring their compliance with both quality and security requirements;

3.2.11 Ensuring and controlling the maintenance of the company's information systems in accordance with the procedure for security and control of information technology systems;

3.2.12 Organizing and developing the technical operation of the company's customer support;

3.2.13 Verification of transfers and other transfers made to comply with instructions;

3.2.14 performing the tasks of the Customer Service Representative as required.

The CEO is also a member of the Management Board, whose suitability is assessed both before starting work and regularly thereafter.

3.3 The duties of the Risk Manager and / or the Head of Compliance are:

3.3.1 Risk management of the company in accordance with the Risk Management Procedure;

3.3.2 Development of the Company's internal rules to ensure that they comply with applicable laws and regulations and that the Company's specific risks are hedged;

3.3.3 Preparation, amendment and supplementation of the Company's Internal Rules in order to comply with the laws, instructions of the regulators and other internal and external regulations concerning the Company's activities;

3.3.4 Introducing the Company's internal rules and procedures to the Management Board and Employees and organizing trainings;

3.3.5 Monitoring compliance with the company's internal rules;

3.3.6 Ensuring the prevention of money laundering and terrorist financing and violation of financial sanctions by the Company;

3.3.7 performance of the duties of the contact person of the Company's Financial Intelligence Unit in accordance with the Company's Internal Rules and applicable legislation;

3.3.8 communication with the Financial Intelligence Unit and other supervisory authorities;

3.3.9 assess the potential impact of any changes in the legal or regulatory environment on the Company's operations and compliance framework;

3.3.10 Performing the duties of a Lawyer / compliance specialist as required;

3.3.11 fulfillment of other obligations arising from the Company's internal rules.

3.4 The tasks of the development manager are:

3.4.1 Attracting investments in the company;

3.4.2 Finding new markets for the company (incl. Performing new markets and analysis necessary for entering them), drawing up an entry strategy and managing entry;

3.4.3 Organizing the company's marketing and marketing;

3.4.4 performing the tasks of the Customer Service Representative as required.

3.5 The duties of a lawyer / compliance specialist are:

3.5.1 Analysis of legislation, instructions, etc. regulating the company's activities;

3.5.2 Preparation, supplementation and amendment of the Company's Internal Rules and similar documents and ensuring their compliance with the legislation regulating the Company's activities, instructions, decisions of the Company's management bodies and similar internal documents, etc .;

3.5.3 Explaining the Company's Internal Rules and similar documents to Managers and Employees;

3.5.4 Preparation of the Company's agreements, incl.

3.5.5 if necessary, advising on the settlement of claims of the Clients and the Company's cooperation partners, including, if necessary, representing the Company in connection therewith;

3.5.6 Advising and assisting the Management Board in preparing meetings and decisions of the company's management bodies (incl. Required documents);

3.5.7 assisting the Management Board in communication with regulators and similar bodies, if necessary.

3.6 The tasks of the accountant (the service is purchased) are:

3.6.1 organization of accounting, including accounting of own funds;

3.6.2 Accurate and timely accounting of the Company's funds and property values and the correct documentation and recording of transactions related to their movement;

3.6.3 ensuring the timely calculation and payment of wages and holiday pay;

3.6.4 calculation, timely transfer and declaration of taxes related to the remuneration of personnel;

3.6.5 preparation of annual reports;

3.6.6 accounting and revaluation of assets and participation in inventories;

3.6.7 Assisting the Management Board in drafting internal accounting rules and other documents in its field;

3.6.8 submitting a monthly report to the Management Board on the financial results of the previous calendar month;

3.6.9 Performing other duties related to the work of the accountant assigned by the Management Board.

3.7 The task of the internal auditor (the service is purchased) is:

3.7.1 identify and assess, in cooperation with the Management Board, risks that affect or may affect the efficiency of the Company's operations and internal control system and, as a result, set priorities for its activities and prepare internal audit work plans;

3.7.2 to check the compliance of the activities of the Company, its Managers and Employees with the applicable legislation, instructions and guidelines of the Financial Intelligence Unit and other supervisory bodies, Internal Rules, decisions and articles of association of the Company's management bodies and to comply with precepts of the Financial Intelligence Unit and other supervisory bodies;

3.7.3 evaluate the management and control measures applied to achieve the Company's objectives, their effectiveness, economy and efficiency, and express an opinion on the adequacy, effectiveness and necessity of these measures;

3.7.4 inform the Management Board, the Company's shareholders and, if necessary, the Money Laundering Information Bureau of its observations and conclusions and, if necessary, make proposals for improving the situation, amending the measures or implementing new ones.

3.8 All Managers and Employees are required to:

3.8.1 thoroughly read the Internal Rules and other internal instructions of the Company;

3.8.2 undergo training introducing the Company's services, Internal Rules, etc .;

3.8.3 act with the foresight and competence expected of them and in accordance with the requirements for their position, proceeding from the interests of the Company and its clients;

3.8.4 to put the economic interests of the Company and its Clients above their personal economic interests;

3.8.5 perform its duties in accordance with the Internal Rules and the law, with sufficient expertise, accuracy and diligence and provide the Customer with the required information about the service.

4 SUBSIDIARIES, REPORTING CHAINS AND REPORTING

4.1 The subordination and reporting chains of Managers and Employees are as follows:

4.1.1 The members of the Management Board are subordinate and accountable to the shareholders of the Company;

4.1.2 the development manager reports to the CEO of the Company;

4.1.3 the lawyer / compliance specialist reports to and reports to the Chief Compliance Officer;

4.1.4 the accountant reports to the Chief Executive Officer of the Company;

4.1.5 the customer service representative (if any) reports to the Chief Executive Officer of the Company;

4.1.6 The internal auditor shall report on his or her activities to the shareholders of the Company, the Management Board and, if required by law, the Financial Intelligence Unit.

4.2 The following principles apply to reporting:

4.2.1 The Management Board reports to the Company's shareholders in accordance with the Commercial Code;

4.2.2 Employees are not obliged to report on their activities periodically, but the Employee is obliged to inform the person to whom he / she is addressed without delay of circumstances that damage or may damage the Company (incl. reputation, financial, etc.) and / or impede or may impede the Company's proper performance. directly subordinates;

4.2.3 The Employee is obliged to report his / her activities to the person to whom he / she is directly subordinate, if the latter requests this from the Employee. The term and form of submission of the report and the content of the report shall be determined by the claimant of the report based on

the purpose of the report and the principle of reasonableness. Employees and Managers shall refrain from making unreasonable reporting requirements;

4.2.4 The Chief Executive Officer has the right to receive reports on their activities in servicing the Clients at any time from the persons who have performed the duties of the Customer Service Representative, including checking the instructions random verification of compliance with the requirements set out in the Internal Rules and legislation in the performance of the Instructions and the performance of other tasks.

5 PROCEDURE FOR DELEGATION OF TASKS

5.1 If necessary, the person or management body to whom the Employee is subordinate shall appoint a substitute for the Employee, taking into account the knowledge, skills and experience necessary for the performance of the Employee's duties.

5.2 The transfer of rights and obligations related to the duties of the Employee is permitted only if the Employee has obtained the prior written consent of the person to whom he or she is directly subordinate.

5.3 The replacement of the manager and the transfer of his / her duties shall be decided by the Management Board.

11. PROCEDURE FOR THE OPERATION OF THE INTERNAL CONTROL SYSTEM

1 PURPOSE

1.1 The purpose of the procedure is to determine:

- the objectives of the internal control system;
- measures taken to perform internal control;
- Procedure for ensuring compliance with the requirements of the Internal Rules and updating the Internal Rules;
- Subordination of employees and managers and reporting procedures;
- procedures for evaluating the effectiveness of the internal control system;
- objectives and scope of internal audit;
- requirements for the internal auditor, procedure for selection and remuneration of the internal auditor, etc .;
- procedures for planning and conducting internal audits;
- the procedure for preparing and submitting the internal audit report;
- the procedure for the storage of internal audit documents and the administration of internal audit;
- compliance with the procedures for the operation of the internal control system and the resulting instructions

2 RESPONSIBILITY

2.1 The Management Board 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

3.1 The purpose of the internal control system is to provide assurance to the Company that:

3.1.1 The company's activities are organized, diligent and purposeful;

3.1.2 The company uses its resources wisely and economically;

3.1.3 the activities of the Company comply with the decisions and articles of association of the management bodies, the Internal Rules and other relevant internal documents of the Company;

3.1.4 The Company's operations comply with applicable legislation;

3.1.5 The activities of the company comply with the precepts of the supervisory authorities;

3.1.6 Risks related to the Company's operations are identified, assessed and minimized in a timely manner;

3.1.7 The company's reporting is true, timely and reliable.

3.2 The company's internal control system consists of the following components:

3.2.1 internal control;

3.2.2 internal audit.

4 INTERNAL CONTROL

4.1 Internal control is performed by the Management Board or a person appointed by the latter. Internal control may not be performed by a person who has carried out the controlled activities alone.

4.2 Internal control is performed on an ongoing basis and no internal control plan is prepared.

4.3 The Management Board shall decide on the appropriate output of internal control on an ongoing basis as necessary, but in any case this output shall be in at least a reproducible form in writing.

4.4 The effectiveness of the internal control system shall be assessed by the internal auditor in accordance with clause 8 of the Procedure.

4.5 The Company applies the following measures to ensure the effective operation of internal control:

4.5.1 establish Internal Rules that comply with the requirements of law and are proportionate, which provide the Managers and Employees with a clear, accurate and thorough overview of the rights and obligations of the Company in providing the Service and performing other activities of the Company;

4.5.2 establishes a procedure that ensures the timely updating of the Internal Rules and compliance with the requirements arising from legislation, and the persons responsible for it;

4.5.3 establishes a procedure that guarantees the proper compliance of the instructions arising from the Internal Rules by the Managers and the Employees;

4.5.4 defines clear subordination relationships and reporting procedures;

4.5.5 determine the procedures for verifying the effectiveness of internal control and continuously evaluate the effectiveness of the internal control system;

4.5.6 adjusts the activity based on the results of the supervision.

4.6 Internal control consists of the following parts:

4.6.1 management control, which consists of work organization, plans, strategy, procedures and practices necessary to achieve the Company's objectives;

4.6.2 administrative control, which consists of procedures and documents related to the decision-making process;

4.6.3 financial control, which includes operations and documentation concerning the preservation of assets, the reliability of financial records and accounting.

4.7 Internal control is carried out in two stages:

4.7.1 ex-ante control, which is a "built-in" system designed to monitor compliance with the Internal Rules, the flow of the Company's financial records and the correctness of financial transactions. The focus of the ex-ante control is on the procedures prior to the transaction and the operation;

4.7.2 ex-post control, which is a check on the correctness and validity of operations and financial transactions that have already been carried out, which is carried out on an ongoing basis (checks are carried out as necessary when deficiencies or problems are identified).

4.8 In the context of ex-ante controls:

4.8.1 Internal Rules shall be drawn up to ensure that both the Managers and the Employees comply with the legislation, precepts of the supervisory authorities, decisions of the management bodies,

etc. and protect the Company's and Customers' property from wastage, misuse, incompetent management and other such damage;

4.8.2 the Internal Rules are periodically updated and supplemented;

4.8.3 trainings are organized for Managers and Employees upon employment and periodically, but at least once a year, during which the Internal Rules are introduced to ensure their observance and integration into daily activities;

4.8.4 collects and maintains true, accurate, timely and reliable information about the activities of Managers and Employees;

4.8.5 transactions performed by the Company are routinely checked.

4.9 In the context of ex-post controls:

4.9.1 assess the adequacy and effectiveness of existing systems and Internal Rules and their integration into the Company's day-to-day business processes;

4.9.2 the compliance of the activities of the Company, its Managers and Employees with the provisions of legislation, precepts of supervisory authorities, Internal Rules, etc. is assessed;

4.9.3 the implementation of budgets, adherence to financial discipline, correct and purposeful use of budgetary and external funds, correctness of the state of accounts, justification of the use of funds, correctness of accounting and reporting shall be assessed;

4.9.4 assess the legality, expediency and efficiency of the use of material values and funds;

4.9.5 the legality, economic expediency and correctness of the performance of the agreements and other transactions entered into by the Company are assessed;

4.9.6 the effectiveness, economy and efficiency of the Company's management and control measures are assessed;

4.9.7 the risks and suitability of countermeasures in the Company's operations are identified and assessed.

5 COMPLIANCE AND UPDATING OF INTERNAL RULES AND PERSONS RESPONSIBLE

5.1 In each of the procedures included in the Internal Rules, the Manager or Employee responsible for its compliance with the requirements and the instructions given by the Managers and the Employees has been determined.

5.2 Each procedure included in the Internal Rules determines which Employees and Managers are obliged to follow the resulting instructions in their activities.

5.3 The internal rules shall be amended and updated and the Managers and Employees shall be notified in accordance with the procedure provided for in the general part of the Internal Rules.

6 SUBORDINATION AND REPORTING

6.1 The highest governing body of the Company is the shareholders' meeting of the Company.

6.2 The Management Board is accountable to the Company's shareholders' meeting, reporting on its activities in managing and representing the Company primarily in the Company's annual report and responding to information requests submitted by the Company's shareholders.

6.3 All departments of the Company are subordinate to the Management Board, i.e. their managers (if any) and Employees. The head of the department reports to the Management Board on the activities of his / her department in accordance with the Internal Rules.

6.4 In departments where there is a head of the department, the Employees working in the department are subordinate to the head of the department. In the absence of the head of the department, the Employee reports directly to the Management Board. The employee shall report on his / her activities (according to whether) to the head of the department or the Management Board in accordance with the Internal Rules.

6.5 The internal auditor is accountable primarily to the Company's shareholders' meeting, but also provides feedback on the results of the internal audit to the Management Board and, if necessary, to the regulator if he or she becomes aware of information about the Company that violates the Client's interests.

6.6 The auditor is accountable to the Company's shareholders' meeting, but also provides feedback on the results of the audit to the Management Board and, if necessary, to the regulator.

6.7 The auditor and the internal auditor shall immediately inform the regulator in writing of any circumstances which have come to their notice which may or may not result in:

6.7.1 Significant violation of the requirements of the legislation regulating the activities of the Company;

6.7.2 Risk of further interruption of the Company's activities;

6.7.3 reverse or annotated sworn auditor's report on the Company's financial statements;

6.7.4 a situation due to which the Company is unable to fulfill its obligations, or a threat of such a situation arising;

6.7.5 Significant property damage to the Company or the Customer arising from the actions of the Manager or Employee.

7 INTERNAL AUDIT

7.1 Definition, scope and consistency of the internal audit activity

7.1.1 The Internal Audit Unit is an independent and objective unit that provides assurance and advice to the Company, is designed to add value to and improve the Company's operations, make proposals to improve the Company's internal control system and contribute to the achievement of the Company's objectives.

7.1.2 The internal audit unit approaches the Company's risk management, assessment of the effectiveness of control and governance processes in a systematic, regular and consistent manner, analyzes the effectiveness of the system and assesses its compliance with the requirements of the applicable legislation.

7.1.3 The company's internal control system must at all times operate independently of internal audit, which does not perform a process-based internal control function in any area or work area.

7.1.4 The performance of internal audit includes the planning of internal audit, the performance of internal audit activities, the preparation of the final report, the communication of results and, if necessary, the follow-up audit or monitoring of results.

7.1.5 The object of an internal audit may be the Company's organizational unit, system, process, operation, function and activities. The object and scope of the internal audit are decided upon the preparation of the Company's strategic internal audit plan and annual work plan.

7.2 Objectives of internal audit

7.2.1 The internal auditor, in cooperation with the Management Board, identifies and assesses risks that affect or may affect the efficiency of the Company's operations and internal control system, and as a result determines the priorities of its activities and prepares work plans.

7.2.2 The internal auditor shall check the compliance of the activities of the Company, its Managers and Employees with the applicable legislation, instructions and guidelines of the regulator and other supervisory bodies, internal rules, decisions and articles of association of the Company's management bodies and monitor compliance with precepts of the regulator and other supervisory bodies.

7.2.3 The internal auditor shall evaluate the management and control measures applied to achieve the Company's objectives, their effectiveness, economy and efficiency and may express an opinion on the adequacy, effectiveness and necessity of these measures.

7.2.4 The internal auditor shall inform the Management Board, the Company's shareholders' meeting and, if necessary, the regulator of his / her observations and conclusions and, if necessary, make proposals for improving the situation, amending the measures or implementing new ones.

7.3 Independence of internal audit

7.3.1 The internal auditor shall be independent in planning his or her activities, determining the scope of the internal audit and conducting the internal audit, and in making observations, conclusions and recommendations and communicating the results, and shall remain neutral with respect to the Company.

7.3.2 In order to ensure the independence of the internal audit, the internal auditor may not be involved in external work tasks that affect the result of the internal audit, including participating in the management of the Company or in the development or implementation of procedures. Consultative activities are permitted.

7.3.3 The internal auditor shall be impartial and open-minded and shall avoid any conflict of interests, that is to say, any situation that may affect the internal auditor's ability to perform his or her duties objectively. A situation of conflict of interest exists even if no unethical or inappropriate act follows. Conflicts of interest may create the impression of inappropriate conduct that could undermine confidence in the internal auditor.

7.3.4 If independence or objectivity is actually or ostensibly impaired, details of the impairment must be disclosed to the Management Board and the Company's shareholders.

7.4 Election and removal of the internal auditor, remuneration

7.4.1 If necessary, the internal auditor shall be appointed and recalled by the Company's shareholders, including the internal auditor's fee, the remuneration procedure and the internal audit budget.

7.4.2 If the Company purchases the services of an internal auditor, the Company's shareholders shall decide on the conclusion, contract and termination of the contract for the provision of the respective service, who shall also elect an authorized representative to represent, enter into and terminate the respective contract.

7.4.3 The service contract with the internal auditor shall be in line with market conditions and shall oblige the internal auditor to comply with relevant legislation, including the Auditing Law and legislation, and all relevant internationally accepted standards and best practices.

7.5 Requirements for the internal auditor

7.5.1 The company's internal auditor may only be a natural or legal person who meets the following conditions:

- he must be honest, trustworthy and have an impeccable professional and commercial reputation;

- have the knowledge, skills, experience, education and professional competence required to perform the duties of internal auditor;

- he must observe professional secrecy and act as an internal auditor;

- he must be objective in his activities and may not hold any post or perform any function which gives rise to or is likely to give rise to a conflict of interests. If the Company purchases an internal audit service, the relevant circumstances and conditions concerning the conflict of interest will be agreed in the respective agreement;

- he must be able to ensure that internal audits are carried out professionally and with due diligence; and

- he must be able to comply with the legislation applicable to the performance of his duties and with internationally recognized standards.

7.6 Risk assessment, planning and conduct of internal audit

7.6.1 Risk is the possibility that a certain situation, event, activity or omission may jeopardize the proper performance of the Company's obligations or the continuation of its activities, or cause the Company to lose its assets or reputation or to achieve its objectives.

7.6.2 Risk assessment is the process of determining the risks affecting the Company, their tolerance limits and priority, and compiling the Company's risk matrix based on the results of such assessment.

7.6.3 The risk assessment shall be carried out before the preparation of the annual work plan for each internal audit.

7.6.4 The provisions of the Company's risk management procedure shall be taken into account in assessing risks.

7.6.5 All levels of the Company's management and the internal auditor are involved in the risk assessment.

7.6.6 In order to plan the activities of the internal audit, the internal auditor shall prepare an annual internal audit work plan for each financial year, which shall be approved by the Company's shareholders.

7.6.7 The annual work plan of the internal audit must be based on the risk assessment, take into account the operational priorities set for them and the resources necessary for the performance of the internal audit, and leave a reasonable reserve for the performance of one-time tasks from the Management Board.

7.6.8 The subject of the internal audit may be any structural units, systems, processes, operations, functions and activities of the Company.

7.6.9 The annual work plan of the internal audit shall contain at least the following information:

- the results of the risk assessments carried out before the annual work plan was drawn up and the priorities set on the basis thereof;

- the objects and objectives of the internal audits to be carried out during the year;

- the duration of each planned internal audit;

- the planned deadline for the completion of each final internal audit report (quarterly);

- the human resources required to carry out each internal audit;

- the resources required to carry out each internal audit, leaving a reasonable margin for possible one-off tasks.

7.6.10 At the request of the Management Board of the Company, the internal auditor shall prepare a corresponding internal audit plan prior to each internal audit, which shall include at least the following information:

- the purpose of the internal audit;

- the name of the audited entity or area;

- the scope and period of the internal audit;

- the time of the internal audit;

- the names of the persons appointed to carry out the internal audit and the division of their responsibilities;

- the stages of the internal audit and their duration.

7.6.11 Rights and Responsibilities of the Internal Auditor in Performing an Audit:

- the internal auditor carries out each internal audit professionally and with due diligence;

- the internal auditor is guided by the legislation applicable to the conduct of each internal audit and the International Standards on Internal Auditing of the Institute of Internal Auditors (IIA), as well as the principles of professional ethics set out in the Code of Ethics;

- The company provides the internal auditor with the working conditions and rights necessary to perform the audit, including the right to receive explanations and information from managers and employees, access to all necessary documentation, all necessary premises and all necessary systems, attendance at meetings considered important by the internal auditor and follow-up. elimination and implementation of the proposals made;

- the internal auditor may, if necessary, involve field experts, assistants or other persons acting under the responsibility of the internal auditor in carrying out the internal audit;

- In performing the audit, the internal auditor shall assess, inter alia:

* The suitability of the company's management framework;
* Relevance of the company's existing policies and activities / procedures and compliance with legal requirements arising from law and international practice;
* Relevance and effectiveness of the applicability of the company's activities / procedures;
* Relevance, quality and effectiveness of the company's three lines of defense;
* Appropriateness and adequacy of the Company's methods (incl. For the prevention of money laundering and terrorist financing) and compliance with the Company's needs and the expectations of supervisory authorities.

7.7 Preparation and submission of the internal audit report

7.7.1 Upon completion of each internal audit, the internal auditor shall prepare a final report setting forth the observations, conclusions and recommendations for improvement made during the internal audit based on the evidence in the audit file.

7.7.2 The internal auditor shall submit the final report to the person (s) responsible for the area subject to internal audit prior to approval for review and comment.

7.7.3 The internal auditor shall approve the final report of the internal audit and submit it immediately to the Management Board and, if necessary, to other executives and shareholders of the Company.

7.7.4 When reporting violations of the law and threats of corruption, the internal auditor shall follow the applicable legislation, as well as internationally accepted standards.

7.7.5 The Internal Auditor shall immediately submit in writing to the Management Board, the Company's shareholders and the regulator any information that has become known to him or her about the Company, which indicates an infringement or damage to the interests of the Clients.

7.8 Internal audit follow-up

7.8.1 After reviewing the internal audit report, the Management Board shall decide on the need to respond to the proposals and observations made therein, if necessary in consultation with the Employees. If there are deficiencies in the activities of the Company, its Managers or Employees or the Internal Rules, the Management Board shall appoint Employees to develop the necessary measures and procedures and / or make corrections to the developed measures and procedures deadline.

7.8.2 The internal auditor assesses the adequacy of the plan based on the nature of the observations made and submits the plan together with his / her comments to the Management Board and the Company's shareholders.

7.8.3 In the event of significant deficiencies in the measures and activities taken to prevent money laundering and terrorist financing, the Company shall submit the relevant internal audit report (s) to the Regulator as soon as possible.
7.8.4 The internal auditor shall perform an ex-post audit no later than 1 year after the preparation of the internal audit report, prepare an ex-post audit report and submit it to the Management Board and the Company's shareholders and, if necessary, to the regulator.

7.8.5 The Management Board shall decide on additional actions on the basis of the follow-up inspection report.

7.9 Retention and record keeping of internal audit documentation

7.9.1 The information obtained during the internal audit, which is the basis for drawing conclusions and recommendations, making recommendations, assessing risks and planning future audits, must be documented and included in the internal audit file.

7.9.2 The internal audit plan and the final report shall also be recorded in the internal audit file.

7.9.3 The internal audit file must ensure that the documents can be easily and logically found in the final report and in the references that may appear elsewhere.

7.9.4 In organizing the administration of internal audit, maintaining and storing the internal audit file, the Internal Rules and legislation regulating administration shall be followed.

7.9.5 The internal audit file shall be kept in electronic or paper form.

12. ENSURING RISK MANAGEMENT AND BUSINESS CONTINUITY PROCEDURE

1 PURPOSE

1.1 The purpose of the procedure is to determine:

- Significant risks associated with the implementation of the company's economic activities;
- Principles of analyzing significant risks of the company;
- Principles for assessing the significant risks of the company;
- The company's significant risk management policies and measures;
- Persons responsible for checking the compliance of the Procedure with the requirements and the proper compliance of the Procedure with the Managers and Employees.

2 RESPONSE

2.1 The Risk Manager is responsible for verifying compliance with the requirements and compliance with the procedure.

2.2 The task of the Management Board is to ensure that the Company has a Business Continuity Plan prepared for the Company's critical business processes.

2.3 The procedure is mandatory for all Managers and Employees.

3 GENERAL

3.1 Risk is defined as a possible negative deviation from the expected financial result or objective.

3.2 The purpose of the company's risk management is to identify, measure and manage risks in a timely manner.

3.3 The provision of the service involves various risks and possible damages, therefore the Company must take appropriate measures to assess and mitigate them.

3.4 In compiling the procedure, the specifics of the Services provided by the Company, the legislation applicable to the Company and the relevant instructions of the regulator have been taken into account.

3.5 In risk management, the Company follows the principle of three internationally recognized lines of defense, where:

3.5.1 The first line of defense, ie the business area, is responsible for risk-taking and day-to-day management;

3.5.2 The second line of defense, compliance check, is responsible for developing and updating risk management methodologies and reporting;

3.5.3 The third line of defense, ie internal audit, performs independent supervision of the entire organization, incl. Risk Management and reports to the Management Board or directly to the Company's owners.

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 Business risk: the risk that inadequate business decisions or inadequate implementation of business decisions or inadequate response to changes in the operating environment and customer behavior or technological developments will result in losses or reduced revenues;

4.1.2 Credit risk: the risk that the Customer is unable or unwilling to meet its contractual obligations to the Company on time or in full;

4.1.3 Liquidity risk: the risk that the Company will not be able to meet its contractual obligations to Customers and partners on time or in full;

4.1.4 Operational risk: the risk arising from the inadequacy or non-functioning of the Company's internal processes, activities of the people or systems involved in the process or external events, such as breaking into the Company's system, stealing Customer data, fraudulent funds;

4.1.5 Strategic risk: the risk arising from an inadequate business strategy or poor implementation of the business strategy.

5 RISK ANALYSIS

5.1 The Company periodically analyzes various possible development scenarios arising from internal and external risk factors when developing its business strategy.

5.2 The Company's Risk Manager shall assess the Company's operational risks, including security risks, related to the Services provided and the adequacy of the security measures and controls implemented to respond to these risks by 1 February of each calendar year at the latest.

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 internal auditor and, if necessary, other Employees are assessed. Particular attention will be paid to the operational and financial risks that have the greatest impact on the Company's continued offering.

6 BUSINESS CONTINUITY PLAN

6.1 In preparing the risk analysis, the Management Board and the internal auditor assess both actual and potential risks, collect relevant information and seek opportunities to ensure the Business Continuity of the Company by preparing a Business Continuity Plan as part of the Risk Analysis.

6.2 The supervisory assessment of the performance of the outsourced essential function shall assess the deterioration or interruption of the quality of performance and the insolvency or other failure of the service provider. The first category of risks is assessed at least once a quarter. All other risks are assessed at least once a year.

6.3 The parts of the business continuity plan are:

6.3.1 Emergency procedures to ensure the safety of all workers;

6.3.2 Functions of information services and roles and responsibilities of support staff;

6.3.3 List of system resources requiring alternatives (hardware, software, etc.);

6.3.4 Priority applications with required recovery times and expected recovery rates;

6.3.5 Recovery scenarios with sufficient detail according to the level of complexity;

6.3.6 List of special equipment needs;

6.3.7 Business Continuity Plan Communication and Training Plans for Employees;

6.3.8 Test schedule;

6.3.9 Details of key persons (name, address, all telephone numbers) with responsibilities and authority to act.

7 RISK ASSESSMENT

7.1 The probability of occurrence of a risk is assessed as follows:

Frequency	Level
one case every 10 years	very low
one case every 3 years	low
one case per year	medium
one case in 4 months	high
one case per month	very high

7.2 The effects of the risks are assessed as follows:

Level	Impact
Low risk	does not interfere with the achievement of the Company's business objectives
Medium risk	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 risk	activities and achievement of goals are significantly disrupted, significant additional resources are needed to achieve the goals
Very high risk	it is not possible to continue activities and / or achieve goals in case of very high risk, elimination of damage requires significant resources

7.3 Risks are divided into three categories based on their probability of occurrence and impact:

7.3.1 Category 1: risks with a high or very high probability of occurrence and a very high or high impact;

7.3.2 Category 2: Risks with a medium, low or very low probability of occurrence but with a high or very high impact.

7.3.3 Category 3: risks with a medium, low or very low probability of occurrence and a medium or low impact.

Within a category, risks are prioritized according to the significance of their effects.

7.4 After assessing and categorizing the risks and their effects, the Company will assess the most appropriate countermeasures to mitigate the specific risks to an acceptable level and, if necessary, arrange for the implementation of countermeasures.

7.5 The acceptable level of risk depends on the risk category and the Company's ability to influence the probability of occurrence of the risk. The levels of tolerable risk are assessed based on the impact of the risks on the interests of the Clients and the Company's business. The more a specific risk affects the interests of the Company's Customers (eg information security issues), the lower the acceptable level of risk.

7.6 Category 1 risks are assessed at least quarterly. All other risks are assessed at least once a year.

7.7 The Company's risk manager shall submit a report on the assessment of the first category of risks to the Management Board at least once a quarter and on the assessment of other risks at least once a year. The report must reflect what risks have materialized, what countermeasures have been taken and proposals for further actions to mitigate the risks. The submission of the report gives the Management Board an overview of the identified risks, an opportunity to assess whether the risks have been adequately defined and whether the measures implemented to mitigate the risks are sufficient or not.

8 RISK MANAGEMENT PRINCIPLES

8.1 The company takes a conservative approach to its business.

8.2 In order to mitigate risks, 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.

8.3 In order to mitigate business risk, the Company regularly updates its business plan, taking into account changes in the market, Customer structure, legal environment, etc.

8.4 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.

8.5 The organizational structure of the Company 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).

8.6 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.

8.7 The Company uses in its economic activities only recognized service providers who have the necessary permits, technical systems and human resources to provide a specific service and who are able to take into account the increased requirements established for the Company when providing the service. If necessary, a service contract will be entered into in accordance with the procedure for transferring the Company's activities.

8.8 The Company's business through a website and a mobile application in the Internet environment is based on customer relationships. Central to the provision of services is the “know your customer” principle, where the extent of customer knowledge must match the results of the risk assessment. The Company assesses the profile of the Clients and the risks involved in concluding the Client Agreements and, if necessary, 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. The Company records and maintains all required data on the Clients and the Instructions issued by them (incl. Operations for monitoring the business relationship or other controls) and ensures the availability of these data to the supervisory authorities.

8.9 The Company uses only such information technology solutions that ensure the security and inaccessibility of the Customer's data to third parties when offering the Service.

8.10 In order to mitigate credit risk, the Company will not execute the Instructions submitted by the Client until the amount necessary for the execution of the Instructions has been received in the respective account of the Company.

8.11 The Company shall keep its funds separate from the funds necessary for the execution of the Instructions transferred by the Clients to the Company and shall not use the Clients 'funds for purposes other than the execution of the Clients' Instructions. The Company holds and invests its funds only in accordance with the Internal Rules, so as to ensure the timely and full fulfillment of the Company's obligations at all times.

8.12 In order to mitigate liquidity risk, the Company programs its information systems in such a way that the responsible Managers and Employees have an overview of all accounts opened in the name of the Company. The Management Board determines the minimum account balance of each account by its decision, and if the account balance of any account falls below the prescribed limit, the Company's information system shall immediately send a corresponding notice to the responsible Managers and Employees. The Responsible Manager or Employee will then promptly take all necessary steps to bring the balance of each Company's account in line with the Management Board's decision - funds will be transferred to the Company's account with more funds than required by the Management Board's decision.

8.13 The Management Board regularly analyzes which accounts are no longer in use and, if necessary, makes a new decision of the Management Board amending the established minimum account balances.

8.14 In addition to the accountant and the Management Board, the financial statements underlying the Company's business are regularly analyzed by the internal auditor and the auditor.

13. INTERNAL ACCOUNTING RULES

1 PURPOSE

1.1 The purpose of the procedure is to determine:

- Basic requirements for the company's accounting and reporting;

- The person responsible for checking compliance with the requirements of the Procedure and compliance with the Procedure.

2 RESPONSIBILITY

2.1 The Management Board and the Accountant are responsible for verifying the compliance of the procedure with the requirements and its proper compliance.

2.2 The procedure is binding on all Managers and Employees, especially the accountant.

3 GENERAL PROVISIONS

3.1 Basics

3.1.1 The accounting principles and presentation of information shall be used in the Company's accounting in accordance with the requirements and basic principles provided for in the Accounting Law in force in the Republic of Lithuania and following the good accounting practice of the Republic of Lithuania.

3.1.2 The Company ensures that it receives current, relevant, objective and comparable information about its financial position, results of operations and cash flows.

3.1.3 If the Procedure does not describe the event occurring in the Company's accounting, the provisions of the Accounting Law in force in the Republic of Lithuania, the guidelines of the Lithuanian Accounting Standards Board and other legislation shall apply.

3.2 Financial year

3.2.1 The Company's financial year begins on January 1 and ends on December 31.

3.2.2 Upon termination of the Company, change of the start date of the Company's financial year and in other cases prescribed by legislation, the financial year may be shorter or longer than 12 calendar months, but in no case shall it exceed 18 calendar months.

3.3 Changing the procedure

3.3.1 The procedure is amended primarily for economic reasons, due to the need to reorganize the Company's work, based on the content of instructions and methodological recommendations issued by the Accounting Department of the Republic of Lithuania and amendments to legislation (especially tax laws and regulations) or for other reasons.

3.3.2 Changes to the procedure shall be made in accordance with the general part of the Internal Rules.

4 DOCUMENTATION AND RECORDING OF TRANSACTIONS

4.1 Accounting entries

4.1.1 The accounting entry must contain the following information:

- the date of the transaction;

- the serial number of the accounting entry;

- the accounts to be debited and credited and the corresponding amounts;

- a brief description of the economic transaction;

- the name and number of the original document (single document).

4.2 Accounting records

4.2.1 The Company's business transactions are recorded in the accounting records at the time of their occurrence or immediately thereafter.

4.2.2 The accounting register shall be drawn up in chronological and systematic order.

4.2.3 Account reports and records are stored on the server and / or printed on paper.

4.3 Source documents

4.3.1 The entry of data in the accounting registers is based on source documents proving economic transactions or consolidated documents prepared on the basis of source documents.

4.3.2 A source document is a written statement confirming that an economic transaction has taken place.

4.3.3 The following source documents shall be used for the calculation:

- invoices (purchase invoices, sales invoices);

- cash receipts, checks;

- cash receipt orders and cash withdrawal orders;

- advance and mission reports;

- payroll documents (consolidated pay slips, pay slips);

- bank statements;

- revaluation and write-off deeds (fixed assets, goods);

- purchase and sale agreements, lease agreements, netting agreements;

- accounting statements;

- inventory sheet.

4.3.4 The source accounting document must contain the following information:

- name and number of the document;

- date of compilation;

- the economic substance of the transaction;

- transaction figures (quantity, price, amount);

- the names of the parties to the transaction;

- the addresses of the parties to the transaction;

- the signature (s) of the person representing the accounting entity recording the transaction, which confirms that the transaction has taken place;

- the serial number of the corresponding accounting entry.

4.3.5 The source document for the regulatory entries made in the preparation of the report is the accounting statement prepared in the accounts. In the accounting certificate, the names and addresses of the parties to the transaction are replaced by the name of the originator.

4.4 Corrections

4.4.1 The information and accounting entries in the source and consolidated accounting documents may not be deleted or corrected without certification.

4.4.2 An incorrect accounting entry shall be corrected by a correction entry, which shall include a reference to the serial number of the accounting entry to be corrected.

4.4.3 If the correction of an accounting entry is not based on the original document, an accounting statement explaining the correction (correction document) must also be prepared.

4.4.4 The person making the correction of the accounting entry shall indicate on the correction document the date of the correction, the signature, the economic content of the transaction and the content of the correction. The previous source document and sentence need to be improved by reference to a later correction document and entry.

4.5 Retention of documents

4.5.1 Accounting records and documents shall be retained for the following periods:

- source accounting documents for seven years from the end of the financial year in which the corresponding source document was entered in the accounts;

- the accounting records, contracts, reports and other commercial documents required for a clear description of the transactions in the audit, for a period of seven years from the end of the financial year in question;

- commercial documents relating to long-term liabilities or rights seven years after their expiry date;

- Repeat seven years after its amendment or replacement;

4.5.2 The following are responsible for keeping accounting records and documents:

- the Board; and

- an accountant.

4.5.3 Accounting records and documents shall be retained in accordance with the following:

- paper documents are stored in an archive cabinet;

- digitally stored documents are stored in appropriate databases and digitally backed up at the end of each working day;

- upon termination of activities, the documents are handed over to the archival institution;

- Upon the transfer of the company or its organisationally independent part, the Company hands over the documents to its successor.

4.6 Document turnover

The source documents of the Company shall compile, check and approve the source accounting documents and submit them to the accountant by the 8th day of the following month at the latest.

5 INVENTORY OF ASSETS AND SETTLEMENTS

5.1 General principles

5.1.1 Inventories are regular and extraordinary.

5.1.2 Regular inventories shall be carried out by the following deadlines:

- inventory of receivables and liabilities - five times a year 31.03; 30.06; 31.08; 30.09; 31.12;

- inventory of assets (fixed assets, inventories and off-balance sheet assets) - five times a year 31.03; 30.06; 31.08; 30.09; 31.12.

5.1.3 The inventory manual shall record:

- scope of inventory;

- reason for inventory;

- the composition of the inventory committee, including the chairman; and

- the date of submission of the final signed results of the inventory.

5.1.4 The accounting officer shall forward the inventory directive to the chairman of the inventory committee and instruct him in connection with the requirements for conducting the inventory.

5.1.5 The chairman of the inventory committee shall notify the other members of the inventory committee of the content of the inventory directive and organize the proper conduct of the inventory.

5.1.6 Extraordinary inventories shall be carried out upon detection of thefts and looting and after a fire (immediately) and a change of materially responsible persons.

5.1.7 Carrying out the inventory is obligatory upon termination of the employment contract and material liability contract with the materially responsible employee (ie the employee is responsible for receiving, storing, issuing or using financial and other material values belonging to the Company in accordance with the material liability agreement).

5.2 Inventory of receivables and liabilities

The inventory of receivables and liabilities is carried out by an accountant, who prepares and sends balance statements to debtors and creditors. A copy of the balance statements shall be retained by the Company.

5.3 Write-down and write-off of receivables and liabilities.

5.3.1 At each balance sheet date, there is an indication that an asset or a liability may be impaired. If any such indication exists, the financial asset is assessed for impairment in accordance with the following rules:

a. Receivables and loans are written down to the present value of expected future payments;

b. Shares and other equity instruments whose fair value cannot be measured reliably are written down to the amount that would be reasonably expected to be obtained if the asset were to be sold at the balance sheet date.

5.3.2 Impairment costs are recognized as an expense in the income statement.

5.4 Inventory of assets

5.4.1 The inventory of assets shall be carried out by a committee of at least three members of the Company formed by the directive of the Chief Executive Officer, the obligatory member of which is the employee materially responsible for receiving, keeping, issuing or using the assets subject to the inventory.

5.4.2 The Asset Inventory Committee shall carry out the counting of goods and materials and enter the results on an inventory sheet, the original copies of which shall be submitted to the accounts and a copy shall be submitted to the materially responsible person. In the event of a surplus or deficit, the materially responsible person shall write an explanatory note.

5.4.3 On the basis of the inventory sheet, the accountant responsible for carrying out the inventories shall prepare a document stating the results of the inventories, the deficiencies or surpluses found.

5.4.4 The Chief Executive Officer of the Company shall make a decision on the amount of compensation to be compensated by the materially responsible Employee and the procedure for compensation by the Accountant in accordance with clause 6.3.3 of the Procedure. on the basis of a document submitted in accordance with Copies of the relevant act shall be provided to the accounting officer and the materially responsible staff member.

5.4.5 Based on the results of the inventory, the necessary accounting entries are made.

6 CASH ACCOUNTING

6.1 The CEO of the Company keeps records of cash operations.

6.2 There is no cash limit, but a minimum amount of cash is kept at the cash desk.

6.3 A cash receipt or withdrawal order is prepared for each cash transaction.

6.4 The cash book shall be kept on a computer and printed out as necessary at least once a month.

7 ACCOUNTING FOR ACCOUNTS

7.1 Accounts shall be opened with credit institution (s), payment institution (s) and companies engaged in virtual currency trading to hold the Company's funds and make settlements and payments.

7.2 General document forms shall be used for settlements - in particular electronic programs through which electronic transfers are made.

7.3 The CEO of the Company and employees with whom the relevant written agreement has been concluded have the right to perform electronic transfers.

7.4 Separate accounts shall be opened for the execution of customer settlements and related settlements (incl. Liquidity reserve recovery entries and bank service fees).

8 CALCULATION OF SHORT-TERM RECEIVABLES

8.1 Receivables from buyers

8.1.1 Settlements with buyers are calculated analytically by invoices and Customers.

8.1.2 Claims denominated in foreign currencies are translated into euros at the exchange rate of the European Central Bank valid on the date of the transaction and are denominated in euros and foreign currencies in parallel. At the balance sheet date, the balance of receivables denominated in foreign currencies is translated at the exchange rate of the European Central Bank ruling at the balance sheet date. Foreign exchange losses or gains are recognized in other operating expenses or income.

8.1.3 Accounts receivable are valued in the balance sheet based on the amounts likely to be received. Invoices not received from buyers, which are unlikely to be received, must be expensed. The probability of receiving each invoice is assessed individually.

8.2 Requirements for reporting persons

8.2.1 Analytical records are kept by reporting persons.

8.2.2 The economic advance is transferred to the bank account of the reporting person or paid out from the cash register. The advance is granted for a period of one month.

8.2.3 Each reporting person is obliged to submit a statement of economic expenses no later than the last day of the calendar month, accompanied by correctly prepared original documents certifying the expenses.

8.2.4 Settlements with reporting persons are kept separate from economic advances.

9 INVENTORY OF INVENTORIES

9.1 The FIFO method is used to determine the acquisition cost.

9.2 Stock balances are obtained from inventory data.

10 ACCOUNTING FOR FIXED ASSETS

10.1 Property, plant and equipment

10.1.1 Tangible fixed assets are assets that are used in their economic activities for a period longer than 1 year and the acquisition cost of which is from 1,000 euros per unit.

10.1.2 Tangible fixed assets are recorded at acquisition cost, which consists of the purchase price, non-refundable taxes and expenses directly related to the acquisition. Land is recorded at acquisition cost.

10.1.3 Tangible fixed assets consist of tangible fixed assets with limited and unlimited use. Depreciation is calculated on property, plant and equipment with limited use. Depreciation is not calculated on fixed assets with unlimited use. Fixed assets with unlimited use are land.

10.1.4 Tangible fixed assets are recorded in the balance sheet at their acquisition cost less accumulated depreciation and any impairment losses.

10.1.5 Costs related to subsequent improvements are added to the cost of property, plant and equipment only if they increase the asset's level of return above the entity's original rate of return. Expenses that restore the object to its original level (such as repairs, maintenance and other similar expenses) are recognized as an expense.

10.2 Intangible assets

10.2.1 Intangible assets include trademarks, patents, licenses, software, rights of use, quotas and other non-physical assets that the Company uses in the production of products, services or for administrative purposes and that it intends to use for more than one year and have an acquisition cost of 1,000 per unit.

10.2.2 Intangible assets are initially recognized at cost, which comprises the purchase price and directly attributable acquisition costs.

10.2.3 Intangible assets are carried in the balance sheet at cost less accumulated amortization and any impairment losses.

10.2.4 Intangible assets are amortized on a straight-line basis over their estimated useful lives of up to 20 years.

10.3 Depreciation calculation

10.3.1 Depreciation is calculated on a straight-line basis.

10.3.2 The asset shall be depreciated from the moment it is put into use and until the depreciable part is fully depreciated or the asset is removed from use. When a fully depreciated asset is used, both the cost and accumulated depreciation are recognized in the balance sheet until the asset is permanently withdrawn from use.

10.3.3 Depreciation of fixed assets is generally calculated on the basis of the following ranges of depreciation rates:

Buildings 2-5% per year; Machinery and equipment 20-30% per year;

Computer technology 20-30% per year; Other tangible fixed assets 20-30% per annum.
10.3.4 In the case of individually significant or non-standard objects, each object must be identified separately
depreciation rate based on the expected useful life of the specific item.

10.3.5 If it becomes apparent that the actual useful life of an asset differs materially from that initially measured, the amortization period should be changed.

10.4 Depreciation of fixed assets

10.4.1 Depreciation of fixed assets that have become unusable shall be made on the basis of depreciation deeds stating the fixed assets:

- name;

- inventory number;

- time and cost of acquisition;

- accumulated expense;

- time and reason for write-off.

10.4.2 The write-off is performed by a commission formed by the directive of the CEO of the Company, the obligatory members of which are the accountant and the person materially responsible for the fixed assets to be written off.

10.4.3 To write off fixed assets, the fixed assets account is credited and the accumulated depreciation account is debited. If the fixed assets become unusable before the entire amount to be written off has been expensed, a loss arises from the liquidation of the fixed assets. The loss is recognized in the income statement as an expense.

11 CALCULATION OF LIABILITIES

11.1 The Company's liabilities are divided into short-term and long-term liabilities.

11.2 Current liabilities are liabilities with a maturity of less than one year. Liabilities that are not short-term are treated as non-current.

11.3 Materially fixed and contingent liabilities, expenses and losses, including the balance of the holiday reserve carried forward to the next financial year, are recorded and recognized as expenses.

11.4 Liabilities denominated in foreign currencies are translated at the exchange rate of the European Central Bank ruling at the balance sheet date of the Company's financial statements.

11.5 Financial liabilities are generally carried in the balance sheet at amortized cost.

11.6 Payroll accounting

11.6.1 The time of calculation of wages, the procedure for payment of wages and terms shall be specified in the rules of internal work.

11.6.2 As a rule, salary payments are not made in cash; on the basis of a written application of the employee, the salary is transferred to the bank account indicated by the employee.

11.6.3 On the date of termination of the employment contract, the employee shall be paid all amounts due. The CEO is responsible for the timely payment of salaries and taxes.

11.6.4 A salary tag shall be prepared for each employee. ID cards are kept on a computer.

11.7 Calculation of holiday pay

11.7.1 Employees shall be paid holiday pay for the period of annual and additional leave in accordance with the legislation in force. The holiday pay shall be paid in full no later than on the penultimate working day before the start of the holiday. The duration of the leave is calculated in calendar days.

11.7.2 The basis for calculating holiday pay for employees is the holiday schedule, which is prepared in the first quarter of each calendar year. The holiday schedule may be changed by agreement of the parties.

11.7.3 The CEO shall submit to the payroll account the documents proving the circumstances regarding the circumstances preventing the use of the leave.

11.7.4 Upon termination of the employment contract, the employee shall be paid financial compensation for unused leave.

11.7.5 The inventory of holiday obligations is made at the end of the year as of 31 December. Unused holiday pay as well as prepayments are recorded in the balance sheet.

12 EQUITY

12.1 The equity of a private limited company consists of:

12.1.1 Share capital - this item is reflected in the nominal value of the Company's share capital;

12.1.2 Reserves - the Company's statutory reserve capital and other reserves are recorded;

12.1.3 Retained earnings (loss) - gains and losses from previous periods that can be used to build up reserves are recognized;

12.1.4 Profit (loss) for the reporting year - the profit or loss generated during the accounting year is recognized.

13 STATEMENT OF REVENUE AND EXPENDITURE

13.1 Income and expenses shall be recognized in the financial statements in accordance with scheme No. 1 of the income statement set out in Annex 2 to the Accounting Law.

13.2 Expenses are recognized in the same period as the related income. Expenses that are likely to contribute to economic benefits in future periods are recognized as an asset when incurred and are expensed in the period in which they generate economic benefits.

13.3 Recognition of revenue from the sale of goods and services

13.3.1 Revenue is recognized at the fair value of the consideration received or receivable.

13.3.2 If the consideration for the goods is received immediately or within a short period after the transaction, the income is equal to the amount of money received or receivable (amounts collected on behalf of third parties are not income of the company).

13.3.3 If the consideration for the goods is received only after a certain period of time, the sales revenue is recognized at the present value of the consideration received.

13.3.4 The difference between the nominal value and the fair value of the consideration receivable is recognized as interest income in the period between the recognition of the sale and the receipt of the consideration.

13.4 Main types of revenue and expenditure

13.4.1 The main revenue is "Revenue from service charges"

13.4.2 The main costs of goods are "Service fees for transactions"

13.4.3 The main operating expenses are "Office expenses"; "Software Usage Costs"; "Advertising Costs";
"Salary and social security expenditure"

13.5 Offsetting Revenue and Expenditure

13.5.1 Income and expenses shall not be offset in the income statement unless the income and expenses arise from the same or a larger number of similar transactions that are not individually significant.

14 REPORTING

14.1 Periodic reporting

14.1.1 The company shall prepare and submit financial statements to the Tax and Customs Board and other state agencies and persons pursuant to the procedure and terms provided for in the Accounting Law and other applicable legislation.

14.2 Annual Report

14.2.1 At the end of the reporting year, it is necessary to perform the following accounting operations:

- inventories of assets and liabilities are carried out and, where necessary, regulatory adjustments are made;

- accrual-based termination entries are made;

- the revaluation of monetary assets and liabilities at the exchange rates of the European Central Bank on 31 December;

- revenue and expenditure accounts are closed;

- an annual report is drawn up.

14.2.2 The annual accounts shall be prepared in accordance with:

14.2.2.1 the Accounting Law and the instructions of the Accounting Standards Board;

14.2.2.2 the balance sheet scheme set out in Annex 1 to the Accounting Law and the income statement scheme No. 1 set out in Annex 2;

14.2.2.3 The notes to the annual report shall be prepared in accordance with Appendix 3 to the Accounting Law.

14.2.3 If, after approval of the annual report, the Company discovers circumstances affecting the previous period that were not reported in a timely manner, the effect of such prior year errors is generally recognized in the annual financial statements.

14. PRINCIPLES OF PROTECTION AND CUSTODY OF CLIENT'S ASSETS

1 PURPOSE

The purpose of establishing these principles for the protection and custody of the Company's client's assets is to provide the principles for the protection and insurance of the Client's assets and the procedure for the operations performed by the Company with the client's assets.

2 RESPONSIBILITY

2.1 The Management Board 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 PROTECTION OF CUSTOMER ASSETS

3.1 In order to provide the service, the Company has accounts specially opened for this purpose in various credit institutions, payment institutions and companies trading in virtual currency. The Company does not use the aforementioned accounts for purposes other than fulfilling the Instructions provided by customers and, if necessary, short-term depositing assets.

3.2 Only the following transactions may be made on the accounts:

3.2.1 Receipt of funds sent by customers;

3.2.2 Return of funds to customers;

3.2.3 liquidity balancing transfers;

3.2.4 other special-purpose transactions not mentioned in the previous sub-clauses (eg transfer of funds in the accounts to ensure the liquidity of the Company's accounts, transfer of service fees paid by the Clients to the Company to the Company's own funds account).

3.3 The Company shall keep the funds of the customer transferred to it by providing the Services separate from the funds related to itself and activities not related to the provision of services.

3.4 All transactions related to other economic activities of the Company, which are not related to the execution of the Instructions provided by the Client, shall be performed using the account provided for this purpose.

3.5 The assets of the clients entrusted to the Company in connection with the provision of the Services belong to the Client related to the provision of the Services and are not included in the Company's bankruptcy assets and the claims of other creditors of the Company are not satisfied.

3.6 The Company collects and stores Customer data in such a way that the Company can immediately distinguish the Customer's assets from the assets of other customers and the assets of customers from its own assets.

4 OPERATIONS WITH CUSTOMER PROPERTY

4.1 The Company shall perform operations with the Client's assets only in accordance with the instructions given by the Client and / or under the conditions agreed in the Client Agreement.

4.2 The Client's property shall not be used for other operations without the Client's respective order.

4.3 The Company shall keep separate records for each Client regarding the Instructions submitted by the Client, the amounts transferred by the Client to the Company and the Instructions executed by the Company.

4.4 If the Customer has made a deposit to the Company's account, but does not submit an order related thereto, the Company shall:

4.4.1 return the paid amount to the person who paid it no later than within 24 hours as of the identification of the person making the transfer; or

4.4.2 deposits the transferred amount until the submission of the respective Instruction by the Client, if the person who made the transfer cannot be identified or contacted or the respective data is incomplete.

4.5 In the case described in clause 5.4.2, the Company shall keep the assets transferred by the client to the Company's account in the Company's special account for up to five years after the receipt of the assets.

4.6 In order to fulfill the obligation specified in clause 5.5, the Company shall create a separate account in which the said funds shall be kept until the identification of the person who made the transfer or for up to five years, whichever occurs first. The assets in such an account are kept separate from the funds of other Clients. After five years, if it is not possible to identify the transferor within that period, the Company includes these funds in its own funds.

4.7 The Company collects and stores data on the operations performed to comply with the Instructions, so that, if necessary, it is possible to identify and verify the operations performed by the Company with the funds provided by the Customer at any time.

4.8 The Company does not invest or deposit funds received from customers. Funds received from customers are stored in special accounts opened in the name of the Company.

5 CUSTOMERS 'PROPERTY INSURANCE

The Client's property entrusted to the Company in connection with the provision of the Service is not covered by an insurance contract or an equivalent security contract.

15. INVESTMENT POLICY

1 PURPOSE

The purpose of this investment policy is to determine the principles of the Company's investment of the Clients and the Company's assets.

2 RESPONSIBILITY

2.1 The Management Board 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 INVESTMENT OF CLIENTS 'ASSETS

3.1 The company does not invest funds received from customers. The funds received from the Clients will be used only to fulfill the Clients' Instructions when consuming the Service.

3.2 The Company holds and protects the Clients' assets in accordance with the "Principles for the Protection and Custody of the Client's Assets" established by the Company's Management Board and applicable legislation.

4 INVESTMENT OF COMPANY ASSETS

4.1 The potential profit earned by the Company shall be invested primarily in the development, improvement and marketing of the Service provided by the Company and the information systems used for its provision and, if possible, in the expansion of economic activities.

4.2 The Company uses the funds received from the owners and investors to develop and conduct the day-to-day business of the Company.

4.3 The Company does not invest its assets in bonds or other similar instruments.

4.4 The company may grant intra-group loans (if it is a group in the future), the detailed terms of which will be decided when the need arises. The Company does not provide loans to other persons.

4.5 The Company may place its funds in deposits only on terms and conditions that allow the funds to be called in without undue delay if necessary (eg to provide or increase liquidity), i.e. to terminate the deposit agreement.

16. PROCEDURE FOR THE COLLECTION OF STATISTICS ON PERFORMANCE, TRANSACTIONS AND FRAUD

1 PURPOSE

The purpose of this procedure is to determine the procedure for the collection of statistical data by the Company.

2 LIABILITY

2.1 The Management Board 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 COLLECTION OF STATISTICAL DATA

3.1 The company collects various statistics as necessary to assess:

3.1.1 the company's current financial results in achieving the set strategic goals;

3.1.2 potential risks related to operations, money laundering, terrorist financing and capital management;

3.1.3 risks related to the customer portfolio, offered services and channels.

3.2 The enterprise collects the following types of statistics:

3.2.1 Number of instructions;

3.2.2 Amounts of instructions;

3.2.3 Currencies and currencies of the Instructions;

3.2.4 Instruction channel;

3.2.5 Geographical location of originators and recipients of instructions;

3.2.6 Instructions by Clients;

3.2.7 Fraud statistics;

3.2.8 Other types of data that are necessary for the Company to fulfill its obligations arising from legislation.

3.3 The statistics to be collected are classified in the Internal Rules section “9. Procedures for the Maintenance of Databases, Processing of Data and Movement of Internal Information and Documents ”shall be applied to the Database and the activities and principles described therein shall be applied in the processing thereof.

17. PROCEDURE FOR PROCESSING PERSONAL DATA

1 PURPOSE

1.1. The purpose of this Procedure for the Processing of Personal Data (hereinafter "the Procedure") is to define:

- what data is collected and processed;

- the legal basis for data processing;

- the purposes for which the data collected are processed;

- how access permissions and the security of internal systems are ensured;

- data retention periods.

2 RESPONSIBILITY

2.1. The requirements set out in this Procedure are mandatory for all Managers and Employees.

2.2. The Management Board is responsible for checking the compliance of the procedure with the requirements and its proper compliance.

3 GENERAL PROVISIONS

3.1. The Company complies with the General Data Protection Regulation[1], the Labour Law, the the Civil Code, the Law on Money Laundering and Terrorist Financing Prevention, the International Sanctions Act, instructions / guidelines of supervisory authorities and other legislation concerning the processing of personal data, as well as the Company's procedures, principles and contract.

3.2. These principles apply to the processing of personal data during the recruitment and selection of employees, during and after the employment relationship, as well as to the processing of personal data of natural persons employed by the Company under employment and agency agreements, unless this is contrary to law or contract.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

3.3. The Company shall limit the processing of Personal Data to the minimum necessary and shall ensure that the collected data is relevant, relevant, accurate and up-to-date and is kept only for as long as is necessary to achieve the purposes set out in this Procedure.

4 GENERAL PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

4.1. Principle of legality

4.1.1. The company ensures that personal data is processed fairly and lawfully.

4.1.1.1. The legal basis for the processing of an employee's personal data is an obligation arising from law or the employee's express consent. Employees have the right to make inquiries about the processing of their personal data.

4.1.1.2. The legal bases for processing the customer's personal data are set out in the privacy policy on the Company's website.

4.2. Principle of purpose

4.2.1. The company processes personal data purposefully. Personal data shall only be processed to the extent necessary to achieve the purpose of the processing. if the consent of the Employee and / or the Client has been obtained for this purpose or if the admissibility of processing arises from legislation.

4.2.2. The undertaking shall, at the request of the competent law enforcement or supervisory authority, provide information, documents and oral or written explanations on the relevant facts.

4.3. The principle of minimum

4.3.1. The Company processes the personal data of the Employees only to the extent that enables the purpose required for the processing to be achieved. Neither the employee nor the customer is obliged to provide the Company with more personal data than is necessary to achieve the purposes of data collection.

4.4. Data quality principle

4.4.1. The personal data processed must be relevant, complete and necessary for the purposes for which they are processed.

4.4.2. The company regularly inspects the data carriers containing personal data in order to determine whether there is a continuing need to store the collected data. The company ensures that the data collected is correct and corrects or deletes outdated and unnecessary personal data.

4.5. Principle of security

4.5.1. The company shall implement appropriate organizational and technological security measures to protect the personal data collected against unauthorized processing, disclosure or destruction.

4.5.2. Access to personal data is guaranteed only to authorized persons.

5 EMPLOYEE INFORMATION

5.1. Personal data processed in the recruitment process

5.1.1. The Company has the right to request from the Candidate only such information that is necessary in the recruitment decision-making phase and for the knowledge of which the Company has a legitimate interest in the circumstances on the basis of which the Company makes the recruitment decision.

5.1.2. In addition to the information published by the Candidate (in the curriculum vitae and motivation letter), the Company performs background checks on public registers and using Internet search engine results, eg publicly accessible social networks, blogs, virtual photo albums, videos (eg Youtube), public registers .

5.1.3. If the employment contract also includes a restriction of competition, the Candidate will be informed (specifying which activities are covered).

In this case, the Candidate will be able to take the requirement into account when assessing whether he has activities that conflict with this condition and decide whether he is willing to give up these activities on behalf of the job offered.

5.2. Employee details

5.2.1. In order to perform the contract, it is important to know the number of the Employee's current account number (where to pay the salary) and contact information (to send applications related to the employment relationship to the Employee or to contact the Employee). In addition, the law stipulates the information that the Company, as an employer, must submit to the Tax and Customs Board, the Labor Inspectorate, the Health Insurance Fund, etc.

5.2.2. Processing of personal data relating to employee leave

5.2.2.1. If the Employee wishes to take additional leave for the parents of minor children, he or she shall provide the Company with documents certifying the Employee's right to parental leave, parental leave for the parent of the disabled child, etc. In addition, the Company requests a written statement from the Employee stating that neither the parent nor the other parent of the child is taking maternity leave or parental leave of the parent of the disabled child with another employer.

5.2.2.2. If the Employee has the right and wishes to take the annual leave of an incapacity pensioner, the Company will also request documents proving the incapacity for work.

5.2.2.3. If the Employee wishes to take study leave, the Company will request a document to prove the student's status.

5.2.2.4. If the Employee is entitled to special leave, the Company will also ask the Employee for the documents on which it is based. In this case, the Company has an obligation to forward the data related to special leave to state authorities, eg in connection with the reimbursement of holiday pay by the state.

5.2.3. The contract between the Company and the Employee includes:

- the employment contract as well as the documents referred to therein (eg organization of work, job descriptions);

- material liability agreement;

- declaration of economic interests;

- an agreement on secrecy and restriction of competition.

The employment contract is characterized by the employee's dependence on the employer. As a result, the Company may inspect the Employee (operations performed in the Customer Environment, e-mails, Internet, compliance with the restriction of competition, renewal of the declaration of economic interests, etc.).

5.2.4. The Company asks the Employee for the name and contacts of a third party with whom the Employee wishes to be contacted in the event of an emergency (such as a sudden illness, etc.).

5.2.5. The employee has the right to receive an extract from the data processed about him. To release personal data, the Employee will contact the Company's (if any) personnel employee. The company is obliged to provide the employee with information and issue the required personal data within five (5) working days following the day of receipt of the respective application. The company issues a copy of the document containing personal data about the Employee or makes an extract

from the document. In the case of electronically stored data, an extract from the information system shall be issued to the Employee.

The employee always has the right to request the correction or deletion of inaccurate and inaccurate data.

6 USING EMAIL AND THE INTERNET

6.1. The employer's e-mail address created for one Employee or containing the Employee's name is the property of the Company and its use for private purposes is prohibited. The company stores content, e-mail exchanges, etc. on work-related devices. The purpose is to prevent the dissemination of trade secrets, damage to IT systems and possible damage to the Company as a result of illegal activities.

6.2. The Company may monitor and investigate the mailbox of the email address provided by the Employer to verify;

- whether the employee's communication is in accordance with the job description and the applicable legal requirements for the respective position, if the fulfillment of the obligation cannot be verified in any other way;

- monitor against fraud.

6.3. An employee is prohibited from storing private items on the Company's hard drive for storing work-related files.

7 HANDLING CUSTOMER INFORMATION AND / OR DATA

7.1. The primary step in processing the Customer Information and / or Data when providing the Service is to obtain the Customer's consent, which is:

- optional;

- concrete;

- aware;

- unambiguous,

A declaration of consent is as easily revocable as given. The Customer must understand that it is not possible to provide the Service to him / her upon withdrawal of the consent. The Client must fill in the Instruction Form to show consent. Electronic consent to execute the Instruction and other commands are stored as logs in the Company's software systems.

7.2. Entering customer data:

7.2.1. The Customer will only be asked for the information necessary for the provision of the Service in accordance with Section “2. Procedure for the provision of the service. Requests for additional information are regulated by the Procedure for the Prevention of Money Laundering and Terrorist Financing and the Application of Financial Sanctions.

7.2.2. Customer data is entered only into the Customer Environment used to provide the Company's Service.

7.2.3. Only the data that the Customer transmits is entered into the Customer Environment.

7.2.4. Silence, pre-filled (checked) boxes and omissions are not considered as consent.

7.3. Once the Instruction Form has been completed, the Client has:

- the right to inspect your data;

- the right to request the correction of data if errors have occurred in the transmission of data;

- the right to withdraw consent.

7.4. If the Customer discovers an error in the submitted data, he / she has the opportunity to correct / change the data. To this end, the Client can make corrections to the Instruction form using the Client Environment.

7.5. Customer data processing:

7.5.1. Customer data is processed lawfully.

7.5.2. The data may only be used for the purpose for which they were collected.

7.5.3. The data entered must be kept exactly as it was transmitted to the Company.

7.5.4. Paper documents must be kept in a locked cupboard or room to which unauthorized access is prohibited.

7.5.5. The data must be up-to-date (eg document validity check at the time of identification)

7.5.6. Personal data will be stored until the purpose of data processing is fulfilled and / or until the term specified by law. In addition, see the Company's data register.

7.5.7. Transmission of customer data by e-mail is prohibited. When sharing data related to the service, only the Customer Environment must be used.

7.5.8. Customer data must be kept secure:

- keep the work environment clean and do not leave documents and papers on the desk when leaving work;

- use of locked cabinets / space for paper data;

- In order to process the data stored in electronic form, the Employee has been given a personal username and password, which is intended only for the Employee and may not be shared with unauthorized persons.

- when leaving the workplace, the Customer Environment System must be locked so that unauthorized persons cannot access or log out; Personal data stored on paper is stored in locked lockers. Access to personal data stored electronically is limited to access rights to information systems.

- When leaving the workplace, the computer screen must be locked;

- Customer data must be stored in the designated location, storage in non-designated locations is prohibited.

7.6. The details of the transaction shall be verified upon issuing the Instruction in accordance with Section “6. Procedures for the Prevention of Money Laundering and Terrorist Financing and the Application of Financial Sanctions ".

7.7. Inquiries arising from the provision of the Service or other general questions related to personal data / forwarded inquiries will be handled by a data protection specialist, who will also manage the e-mail address compliance@Quan2um.pro.eu.

7.8. Steps to handle a customer request:

7.8.1. Identify the Person / Customer.

Application requirements:

- First and last name;

- personal identification code / date of birth;

- Phone number;

- E-mail address;

- Content of the application;

- Date of application;

- Request for signature confirmation.

7.8.2. Upon receipt of the request, the Data Protection Officer shall assess the content and consequences of the request.

If necessary, the data protection specialist shall explain the consequences to the Customer if, for example, the execution of the request is not possible (eg the storage of the original data of the transaction arises from the law when deletion is not possible within 7 years).

If partial deletion of data is possible, the data protection officer will find out which data can be deleted from the whole, what the consequences are, and so on.

8 INTERNAL SYSTEMS, MOBILE DEVICES (LAPTOPS AND OTHER DEVICES)

8.1. Internal systems used in the company

8.1.1. The company uses the Google drive system as a work environment, where the Employee is granted access only to those files that are necessary for the performance of the tasks specified in the employment contract.

All documents are connected to Google Drives https and encrypted, including all external systems. As a result, data security is ensured in the case of remote work, when, for example, when using a work computer outside the office or using a foreign Wi-Fi network, all information is in an unreadable form to an unauthorized person (eg in the case of hacking). In addition, the use of Google Accounts or drive on other devices is protected by 2x authentication, etc.

8.1.2. The Company has put in place procedural and technological measures to ensure that the collection, routing, processing, storage and / or archiving and visualization of transaction data is adequate, appropriate and limited to what is necessary to provide the Service.

8.1.3. The users of the service delivery system are divided into different categories according to the rights granted to the users. In this way, access to unnecessary data is restricted on a user-by-user basis and unauthorized operations in the system are prevented.

8.2. Customer environment

8.2.2. Access to the Customer Environment is granted only to the relevant persons who have a requirement / right to perform the Service arising from law or contract. Access to other information systems is restricted to authorized persons, such as for regular security checks of the systems, etc.

8.2.3. The granting of access rights shall be based on the principle that the rights granted to a person shall be limited to that part of the rights which is necessary for the individual. The right of access is role-based.

Recipients of system access rights have a personal user ID and password. Repeat access attempts are restricted, the user will be blocked after the sixth attempt. After 15 minutes of inactivity, the system will lock automatically. You will then be prompted to log in again with your username and password.

8.2.4. Only data related to personal identification and the Instruction will be entered into the customer environment. The principle of minimum is followed, when upon performance of the Service, only the following information is provided to the counterparty, which is necessary for the final execution of the transaction:

- Name of the originator of the instruction;

- Name of the beneficiary;

- Amount;

- Explanation of the transaction

9 PROCEDURES FOR STORAGE OF PERSONAL DATA

9.1. Personal data shall be stored only for as long as is necessary for the fulfillment of the purpose or as long as the storage of the data is required by law or contract. The corresponding data retention periods are defined in the data register.

9.2. Purpose:

- minimize the time of storage of personal data, while ensuring that the Company's information needs are met;

- ensure that the documents required for legal and evidentiary purposes are kept for an appropriate period and in an appropriate manner;

- ensure that documents are not destroyed prematurely.

9.3. This personal data retention policy applies to all processors and managers of data related to the Company (documents, copies of identity documents, Instructions, employment contracts, etc.). Based on the purposes of the data processing and the legal basis, the term of data retention is set out in the Company's data register.

10 DATA PROTECTION TRAINING

Data protection training is provided on a regular basis, but not less than once a year. If there are changes in the legislation, the structure of the Company, the training will be carried out as needed.

11. SUMMARY

DATA SUBJECT GROUP	TYPES OF PERSONAL DATA	BASIS FOR PROCESSING	RETENTION PERIOD
Job applicants	Name, motivation letter, personal data provided in the CV	Consent (has provided the Company with personal data), legitimate interest	Until the conclusion of the employment contract, notification of the unsuccessful application
Job applicants	Background check: eg valid criminal records and only for offenses that are relevant for the post	Legitimate interest	Until the conclusion of the employment contract, notification of the unsuccessful application.
Employees (including members of the management board)	Name, personal identification code, contact details, salary details	Employment contract (for performance of the contract), legal obligation	Retention period provided for in the reporting obligation and retention period of accounting documents
Employees (including members of the management board)	Diplomas, other certificates, documents on which the special leave is based	The need to prove to third parties the right of an employee to obtain a qualification or special leave.	Until the end of the employment contract (copies)
Partners and other relevant persons	Name, contact information, e-mail address	Consent, contract, legitimate interest	According to the purpose
Senders/recepients of funds	Name, contact details, document details, background check details and other necessary additional information pursuant to AML/CTF Law	Consent, Transaction, AML/CTF Law	5 years after the execution of the Instruction. At the written request of the Financial Intelligence Unit, this data may be kept for an additional period of up to 5 years.
Senders/recepients of funds	Transaction related data: amount, currency, country of destination, etc.	Consent, payment order	7 years from the end of the financial year of the respective executed Transactions
People involved in provision of legal advice and litigation	Name, contact details, other necessary data as appropriate	Consent, contract (represented), preparation, submission or defense of a legitimate interest and legal claim (special type of personal data).	Depending on the situation (eg termination of litigation at all possible levels, termination of the right of representation).
Persons contacted via means of e-mail and other	Name, contact details	Consent (is the Company 's personal data Is shared)	According to the purpose
Research subjects	According to the purpose and needs of the study	Consent, legitimate interest	According to the study design and needs
Research subjects	Name, e-mail address, information about interaction	Consent	Regular opt-out reminder

Proceedings participants	Name, contact information, fact of participation in the proceedings	Legal obligation (list of participants)	Retention period required by the reporting obligation

* Certain data will be kept by the Company for some time inactive use, eg in case of possible disputes (data concerning the subject matter of the dispute)

12 ANNEX 5. CODE OF CONDUCT FOR BREACHES OF PERSONAL DATA

1. A personal data breach is any breach of security which involves the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. All questions, inquiries, requests for deletion / modification, etc. related to personal data, including violations, will be forwarded to the e-mail address kabirul@gmail.com.

2. In the event of a personal data breach which poses a serious threat to the fundamental rights and freedoms of the data subject, the Company's data protection officer shall, as soon as it becomes aware of the breach:

2.1. The supervisory authority - The Data Protection Inspectorate must be notified if a leak poses a serious threat to a person's fundamental rights and / or freedoms. These are leaks of data that cause personal identity or potential material damage. The AKI must also be notified if the data leak has been massive. For example, the entire customer database has fallen victim to ransomware. In both cases, you must notify AKI of the violation within 72 hours.

2.2. The person himself, if the violation is likely to endanger the fundamental rights and freedoms of the person. For example:

- interference with life and health; for example, documents containing health information leak to the wrong people.
- invasion of privacy: eg contact details with a history of money transfers have been leaked. The result is profiling a person by strangers, spam and uncontrolled resale of data.
- Infringement of honor and reputation: eg a slacker account has been created for a person on the adult portal with his / her correct contact details. There is no control when creating an account on the portal (the added e-mail address and telephone number are under the control of the account creator).
- Obstacle to free self-realization and freedom of enterprise: eg embarrassing misinformation about a person is widespread, which has prevented him or her from operating successfully.
- Obstacle to the freedom to choose an activity, profession and job: eg the information system has destroyed a person's education data, which prevented him / her from applying for the desired job in time.

3. Immediate notification of the violation also applies to the processor authorized by the Company (cooperation partners, etc.).

4. The notice shall indicate which data files were lost, how many persons are affected by the leak, and describe the possible consequences and measures taken by the Company to deal with the breach.

5. The infringement notification shall contain the following information:

5.1. A description of the nature of the personal data breach (eg loss, destruction, theft, copying, unauthorized alteration, reading or transmission).

5.2. Where possible, the categories and approximate number of data subjects concerned and the types and approximate number of relevant personal data records. Examples of categories of data subjects are: residents, non-residents, enterprise, employees, etc. Examples of types of personal data are: name, user ID, means of communication, history of instructions, details of indebtedness, etc.

5.3. Name and contact details of the data protection officer (responsible person) or other contact person.

5.4. Description of the possible consequences of the personal data breach.

5.5. A description of the measures taken to address the personal data breach, including, where appropriate, the mitigation of the possible harmful effects of the breach.

6. All personal data breaches shall be documented and recorded by the compliance unit. The circumstances of the breach as well as its effects and the corrective measures taken shall be documented.

7. The risk manager shall, at least annually, provide the compliance officer with an overview of non-compliances, the effectiveness of mitigation measures and further action plans to prevent similar incidents.

This document forms the compliance policies of Xazur Technologies UAB

Date 21/11/2022

Signed Mr H Bedi
Designation Director

Signature