crowdpear

Business Centre ELEVEN,
Kareiviu str. 11B, LT-09109
Vilnius, Lithuania

Crowdpear, UAB
+370 615 54424
info@crowdpear.com

MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION POLICY

1. GENERAL PROVISION

1.1. The present Money Laundering and Terrorist Financing Prevention Policy ("**Policy**") of UAB Crowdpear ("**Company**") determines:

1.1.1. The Company's client identification and transaction monitoring procedures; and

1.1.2. The money laundering and terrorist financing prevention measures used and applied in the Company's activities when the Company administers the crowdfunding platform "Crowdpear".

1.2. The Policy also describes the procedures for assessing the Company's entire activities and individual money laundering and terrorist financing risks, as well as specific functions related to the prevention of money laundering and terrorist financing and the persons responsible for the implementation of these functions.

1.3. The Manager of the Company is responsible for the Policy implementation in the Company. The Responsible Person appointed by the Manager of the Company is responsible for the implementation of specific functions provided for in the Policy.

1.4. The Policy has been prepared in accordance with the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania and other applicable legislation.

2. DEFINITIONS

2.1. Unless the context requires otherwise, the capitalised definitions used in this Policy have the below meanings:

2.1.1. **Close Associate** – the close associate means:

2.1.1.1. a natural person who is a participant of the same legal entity or an organization that does not have the status of a legal entity or maintains other business relations with the Politically Exposed Person;

2.1.1.2. a natural person who is the sole owner of a legal entity or an organization without legal entity status, established or operating de facto for financial or other personal benefit to a Politically Exposed Person.

2.1.2. **Family Members** – the spouse, the person with whom partnership has been registered (hereinafter: the "cohabitant"), parents, brothers, sisters, children, children's spouses and children's cohabitants;

2.1.3. **Responsible Person** – the person appointed by the Manager of the Company responsible for the implementation of the money laundering and/or terrorist financing prevention measures provided for in the present Policy in the Company's activities;

2.1.4. **Company** – UAB Crowdpear, code of legal entity 305888586, seat address: Kareivių g. 11B, Vilnius, Lithuania;

2.1.5. **FCIS –** the Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania;

2.1.6. **Law** – the Law on Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania;

2.1.7. **Client –** a natural or legal person who uses the services provided by the Company through its managed crowdfunding platform "Crowdpear";

2.1.8. **Beneficiary** – a natural person who is the owner of the Client (a legal entity or a foreign state company) or who controls the Client, and/or a natural person on whose behalf the transaction or activity is carried out. The beneficiary is:

2.1.8.1. In the legal entity:

1) a natural person who owns or controls a legal entity, directly or indirectly with a sufficient percentage of the shares or voting rights of that legal entity, including control through bearer shares, with the exception of joint stock companies or collective investment entities whose securities are traded on regulated markets, where requirements to disclose information about their activities complying with European Union legislation or equivalent international standards are applied, or by controlling it in other ways. A natural person who owns 25 percent and one share or more than 25 percent of the ownership of the Client is considered a direct owner. A natural person(s) controlling a company or several companies that owns 25 percent and one share or more than 25 percent of the Client's ownership is considered the indirect owner(s);

2) a natural person holding the position of a senior manager, if the person referred to in point 1 has not been identified or if there are doubts that the identified person is a beneficiary;

2.1.8.2. In the trust funds – all these persons:

1) Trustee(s);

2) Trustor(s);

3) Guardian(s), if any;

4) Natural persons receiving benefits from a legal person or entity without legal person status, or, if these persons have not yet been identified, the persons for the representation of whose interests that legal person or entity without legal person status is established or operates;

5) Any other natural person who effectively controls the trust fund through direct or indirect ownership or other means;

2.1.8.3. In the legal entity that administers and distributes the funds, an entity similar to a trust fund – a natural person holding the position equivalent to specified in the Clause 2.1.7.2 of the Policy.

2.1.9. **Monetary Transaction –** any payment, transfer or receipt of money;

2.1.10. **Money Laundering**:

2.1.10.1. The change of the legal status of assets or transfer of assets knowing that these assets are the proceeds of a criminal act or participating in such an act to conceal or disguise the illegal origin of the assets or to help any person involved in a criminal act to avoid the legal consequences of such activities;

2.1.10.2. The conceal or disguise of the true nature, true origin, source, location, disposition, movement, ownership or other rights associated with the assets, knowing that the assets are the proceeds of a criminal act or participating in such an act;

2.1.10.3. The acquisition, management or use of the assets knowing that these assets were obtained from a criminal act or participating in such an act at the time of acquisition (transfer);

2.1.10.4. The preparation, attempt to commit and complicity in doing any of these actions specified in the Clauses 2.1.10.1 – 2.1.10.3 of the Policy.

2.1.11. **Policy** – the present document;

2.1.12. **Third Country –** the state that is not a Member State;

2.1.13. **Third Party –** the financial institution, another obliged entity or a financial institution or other obliged entity registered in a Member State or in Third States under the supervision of competent authorities meeting the following requirements:

2.1.13.1. They are subject to mandatory professional registration established by law;

2.1.13.2. They are registered in a Member State or a Third Country that applies requirements equivalent to the requirements for identifying the clients and beneficiaries and information storage requirements set by the European Union, and are supervised by the competent authorities for compliance with these requirements.

2.1.14. **Member State** – the country that is a member state of the European Union or the European Economic Area;

2.1.15. **Politically Exposed Persons (PEP)** – the natural persons who are (or have been in the last 12 months) entrusted with Important Public Positions, as well as their Family Members or Close Associates;

2.1.16. **Important Public Positions** – the positions in the Republic of Lithuania, the European Union, international or foreign institutions:

2.1.16.1. The head of State, head of Government, Minister, Vice Minister or Deputy Minister, Secretary of state, Chancellor of Parliament, Government or Ministry;

2.1.16.2. The member of the Parliament;

2.1.16.3. The member of supreme courts, constitutional courts or other supreme judicial institutions whose decisions cannot be appealed;

2.1.16.4. The mayor of the municipality, director of municipal administration;

2.1.16.5. The member of the management body of the highest state audit and control institution or the Chairman of the Board of the Central Bank, his/her Deputy or a Member of the Board;

2.1.16.6. The ambassador, temporary chargé d'affaires, Commander of the Lithuanian Army, commanders of military forces and formations, chief of the defence staff or high-ranking officer of the armed forces of foreign countries;

2.1.16.7. The member of the management or supervisory body of the state-owned company, joint-stock company, closed joint-stock company whose shares or part of shares providing more than 1/2 of all votes in the general meeting of shareholders of these companies belong to the state by the right of ownership;

2.1.16.8. The member of the management or supervisory body of the municipal company, joint-stock company, closed joint-stock company whose shares or part of shares, providing more than 1/2 of all votes in the general meeting of shareholders of these companies belong to the municipality by the right of ownership and which are considered large companies according to the Law on Financial Reporting of Companies of the Republic of Lithuania;

2.1.16.9. The head of an international intergovernmental organization, his/her deputy, a member of the management or supervisory body;

2.1.16.10. The head of a political party, his/her deputy, member of the governing body;

2.1.17. **Terrorist Financing** – an act constituting an offense according to the Article 2 of the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999;

2.2. Other definitions used in the present Policy are understood as defined in the Law, the Law on Crowdfunding of the Republic of Lithuania or other legislation applicable to the Company.

2.3. It must be noted that the definitions Terrorist Financing and Money Laundering may also be used in this Policy in lowercase.

3. IDENTIFICATION

3.1. It is important for the Company's employees to know the identity of their Client and Beneficiary, therefore the Company follows the principle "*Know Your Customer*" in its activities. The employees of the Company determine and verify the identity of the Client and Beneficiary in all cases:

3.1.1. Before starting a business relationship;

3.1.2. Where there are doubts about the correctness or authenticity of the previously received identity data of the Client and Beneficiary;

3.1.3. Where there are suspicions that money laundering and/or terrorist financing is, has been or will be carried out, regardless of the amount of the Money Transaction or other exceptions.

3.2. In its activity, the Company:

3.2.1. Does not carry out the transactions and/or operations, does not start and/or does not continue the business relations with the Clients whose identity and Beneficiary's identity cannot be properly determined and verified, i. e., if the Client in the cases specified in the Policy:

3.2.1.1. Does not provide its identification data;

3.2.1.2. Avoids providing identification information and data, provides incomplete or incorrect data;

3.2.1.3. Does not provide the Beneficiary‘s identification data;

3.2.1.4. Avoids providing the Beneficiary identification information, provides incomplete or incorrect data, or the data provided is insufficient to identify the Beneficiary;

3.2.1.5. Does not provide the information and data necessary to identify the Client and the person on whose behalf this Client acts, in case of starting business relations and performing operations through a representative;

3.2.2. Does not start and/or does not continue the business relations, does not carry out the transactions, when the Company's employees cannot fulfil the requirements of the present Policy or the Law for the Prevention of Money Laundering and/or Terrorist Financing.

3.3. The Company is not responsible to the Client for non-fulfilment of contractual obligations and damage caused due to non-fulfilment of the Client's monetary transactions or arrangements, if the Company did not fulfil the Client's monetary transactions or arrangement for the reasons specified in Clause 3.2 of the present Policy.

3.4. The Company must apply the identification measures of the Client and Beneficiary not only to new but also to existing Clients by taking into account the level of risk, in the event of new circumstances or the emergence of new information related to the determination of the level of risk of the Client, the Beneficiary, their identity, their activities and other significant circumstances.

4. INITIAL IDENTIFICATION

4.1. The Client and the Beneficiary can be identified by the Client's physical presence or remotely, i. e., without the Client‘s physical presence.

4.2. The initial identification of the Client and the Beneficiary is carried out when the data about the Client, Beneficiaries and the Client's representatives are received for the first time.

4.3. All information collected during the initial identification is stored on electronic media (Client’s file).

5. IMPLEMENTATION OF CLIENT AND BENEFICIARY KNOWLEDGE REQUIREMENTS

5.1. Before starting a business relationship, identifying and/or verifying the identity of the Client and Beneficiary, the employees of the Company carry out the following actions:

5.1.1. Receive the documents certifying the identity of the Client with the data about the Client and the Beneficiary from the Client;

5.1.2. Determine the required data about the principal and the representative, when a monetary transaction is carried out or an arrangement is concluded through a representative;

5.1.3. Receive the information allowing to understand of the purpose and expected nature of the business relationship between the Client and the Beneficiary clearly;

5.1.4. Receive the information allowing to understand the Client's (legal entity‘s) management structure, activities and expected nature of business;

5.1.5. Verify the information received from the Client based on the documents, data or information obtained from a reliable and independent source:

5.1.5.1. The official documents containing:

1) In case of natural persons – the personal photograph and/or corresponding registration number that cannot be easily copied or forged (passport, personal identity card, driver's license issued by the country of the European Economic Area, extract from the Register of Legal Entities, notarised copies of the documents) with Client‘s name, surname, personal identification number or other unique sequence of digits to identify the person, citizenship, personal photograph and/or signature, etc.;

2) In case of legal entities – name, legal form, address, code, registration certificate number, VAT payer’s code, etc.;

5.1.5.2. The publicly available information and information obtained from the databases (such as the Register of the legal Entities, information system of participants of legal entities, etc.).

6. IDENTIFICATION BY PHYSICAL PRESENCE OF THE CLIENT

6.1. During the Client identification by its physical presence, the employees of the Company submits the form established by the Company to fill by the Client. When filling in the form, the Client must provide the accurate data and answer the questions specified in the form properly and fully. If the employees of the Company determine (or have doubts) that the Client provided incomplete information in the questionnaire, the employees of the Company must immediately ask the Client to properly fill in all relevant fields specified in the form.

6.2. The company's employees always require an identity document of the Republic of Lithuania or a foreign country, a residence permit in the Republic of Lithuania or a driver's license issued in a country of the European Economic Area from the Client (natural person) with the following identification data:

6.2.1. name (names);

6.2.2. surname (surnames);

6.2.3. personal code (in case of foreigner – date of birth (if available - personal code or other unique sequence of characters assigned to this person for his/her identification), number and validity period of the residence permit in the Republic of Lithuania, place and date of its issuance (applicable to the foreigners);

6.2.4. photograph;

6.2.5. signature (except for cases where it is optional in the identity document);

6.2.6. citizenship (except for cases where it is optional in the identity document), if the person is stateless - the state that issued the personal identification document.

6.3. During the identification of the Client – legal entity, the employees of the Company require its identity documents or copies of these documents with a notary's certificate confirming the authenticity of the copy of the document with the following data:

6.3.1. name;

6.3.2. legal form, seat (address), actual business address;

6.3.3. code (if the code is provided);

6.3.4. registration extract and its issuance date.

6.4. When starting the identification of the Client, the employee of the Company must:

6.4.1. Assess whether the Client (or Client‘s representative) – natural person – starting the cooperation with the Company, submits the valid documents specified in the Clause 6.2 of the present Policy; to determine whether the document submitted by him/her contains a photo of that particular Client;

6.4.2. Assess the condition of the submitted document (pay particular attention to whether the photo, pages or records have not been changed, corrected, etc.);

6.4.3. Find out whether the Client will use the Company's services by himself/herself or whether he/she will represent the interests of another person;

6.4.4. Verify whether the natural or legal person has the necessary authority to act on behalf of the Client;

6.4.5. Make a copy of the pages of the document specified in the Clause 6.2 of the present Policy containing the photograph or other data necessary for identification of this natural person or scan the document. Having made a copy of the document, the employee of the Company must put a mark of authenticity (the mark of authenticity consists of the words “Copy true“, position, signature, name and surname of the employee, date and the Company's seal, if the Company is required to have it) on each copy of the document confirming the identity of the Client (if a paper copy of the document is made);

6.4.6. Verify whether there are circumstances to apply an enhanced Client identification properly;

6.4.7. Add the necessary data about the Client, his/her representative and the Beneficiary to the Company's databases and place the documents in the Client's file.

6.5. Where the Client is a legal entity represented by a natural person, or the Client - a natural person is represented by another natural person, the identity of these representatives is determined in the same way as the Client - a natural person. The Client must provide the Company with information about the manager of the legal entity: name, surname and personal code of the manager (in case of foreigner – date of birth (if available, – personal code or other unique sequence of characters assigned to this person for identification purpose), citizenship.

6.6. Where the Client is a legal entity represented by a natural person, or the Client - a natural person is represented by another natural person, the Company's employees must request a power of attorney and verify its validity (i. e., the right of the person who issued it to issue such power of attorney), validity period of the power of attorney and the performed actions specified in the power of attorney (the power of attorney must meet the requirements of the Civil Code of the Republic of Lithuania). A power of attorney issued abroad must be legalized or confirmed by a document approval certificate (*apostille*).

6.7. If the Client, who is a legal entity, is represented by another legal entity or natural person and the basis of such representation is determined in the Client's founding documents, the Company's employees must check the document appointing the person to the relevant management body of the Client and get acquainted with the part of the Client's founding documents (Articles of Association, etc.) confirming such facts or get acquainted with an extract from the register confirming that the person has the right to act on behalf of the Client.

6.8. Each time starting a business relationship with the Client, the employees of the Company obligatorily inform the Client of its obligation to immediately inform the Company in writing of the cancellation, expiration or change in the scope of its representative's authority. Prior to provision of such information to the Company, it is considered that the representative's authority has not expired, unless the Company knew or should have known about the cancellation, expiration or change in the scope of the Client’s representative's authority.

7. CLIENT IDENTIFICATION WITHOUT ITS PHYSICAL PRESENCE

7.1. The Company identifies the Client without its physical presence by using electronic means that allow live video transmission in one of the following ways:

7.1.1. Using Third Party information about the Client or the Beneficiary;

7.1.2. Using electronic identification means issued by the European Union and operating according to electronic identification schemes with a high or sufficient level of security assurance, set forth by the Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

7.1.3. Using a qualified electronic signature certificate that complies with the requirements of the Regulation (EU) No. 910/2014 where the information about the personal identity is confirmed with a qualified electronic signature. The qualified electronic signatures of Third Countries created using a qualified electronic signature certificate are recognized in accordance with Article 14 of the Regulation (EU) No. 910/2014;

7.1.4. Using the electronic means enabling live video transmission in one of the following ways:

7.1.4.1. During the live video transmission, the original document identifying the Client is captured and the Client's identity is confirmed using an advanced electronic signature complying with the requirements of the Article 26 of the Regulation (EU) No. 910/2014;

7.1.4.2. During the live video transmission, the image of the Client’s face and the original of the identity document shown by the Client are captured.

7.2. If the Client and Beneficiary are identified in cases specified in the Clauses 7.1.1 – 7.1.3 of the present Policy, the Company must comply with the following conditions:

7.2.1. Prior to identification of the Client and Beneficiary in cases specified in the Clause 7.1.1 – 7.1.2 of the present Policy, the Third Party identified the Client by its physical presence or through the use of electronic means allowing live video transmission in one of the methods specified in Clause 7.1.4 of the present Policy, as well as when the Client‘s identity was established by its physical presence during the issuance of an electronic identification device operating according to an electronic identification scheme with a high or sufficient level of security assurance;

7.2.2. Prior to identification of the Client and Beneficiary in cases specified in the Clause 7.1.1 – 7.1.3 of the present Policy, the Client and the Beneficiary – the representative of the natural person and the legal entity – were identified in the cases specified in the Article 9 of the Law from the documents specified in the Article 10 of the Law.

7.3. If the Client is identified without its physical presence, the Company must take the measures provided for in Chapter 3 of the present Policy, identify and verify the identity of the Client and the Beneficiary, use the additional data, documents or additional information that would allow to verify the authenticity of the Client's identity to identify the Client and the Beneficiary, and check whether there are circumstances to apply enhanced identification of the Client.

7.4. The Company may use the Third Parties and their offered technological solutions to identify the Client without its physical presence. In such case, the Company ensures that all information collected during the identification of the Client and Beneficiary is transferred to the Company and stored in the Client's file. In addition, The Company stores the information collected during the live video transmission, the information of the Client verification collected in the international financial sanctions lists and lists of politically exposed persons in the Client‘s file.

7.5. During the Client‘s identification, the Company may also use the services of Third Parties and the information provided by them. Prior to identification of the Client and the Beneficiary based on information from Third Parties, the Company must ensure that:

7.5.1. The Third Party has identified the Client in one of the following methods:

7.5.1.1. By its physical presence from the personal identification documents, extract from the Register of Legal Entities or establishment documents of the legal entity;

7.5.1.2. Using the electronic means that allow live video transmission;

7.5.1.3. By making a payment to a Third Party's payment account on behalf of the Client from the account in a credit institution registered in a Member State or a Third Country that has established requirements equivalent to the requirements of the Law and is supervised by the competent authorities for compliance with these requirements, and by submitting a paper copy of the personal identity document approved in the manner established by the legislation of the Republic of Lithuania;

7.5.2. Upon the Company's request, the Third Party will provide all requested information and data that must be held in accordance with the requirements for identification of the Client or Beneficiary specified in the Law and Policy immediately;

7.5.3. Upon the Company's request, the Third Party will provide the copies of documents related to the identification of the Client or Beneficiary and other documents related to the Client or Beneficiary that must be held in accordance with the requirements for identification of the Client or Beneficiary specified in the Law and Policy immediately.

7.6. When selecting a Third Party whose information will be used to identify the Client and the Beneficiary, the Company takes into account the fact that the Company is responsible for the compliance with the Client or beneficiary identification requirements of in the Law and Policy.

8. BENEFICIARY IDENTIFICATION

8.1. During the Client identification, it is mandatory to identify the Beneficiary(-ies) in all cases. In all cases, the Beneficiary identification means the identification of a natural person or group of natural persons.

8.2. During the identification of the Beneficiary, the employees of the Company must request the Beneficiary's identification data from the Client:

8.2.1. name (names);

8.2.2. surname (surname);

8.2.3. personal code (in case of foreigner – date of birth (if available - personal code or other unique sequence of characters assigned to this person for his/her identification), number and validity period of the residence permit in the Republic of Lithuania, place and date of its issuance));

8.2.4. citizenship (if the person is stateless - the state that issued the personal identification document).

8.3. The employees of the Company verify the documents and information about the Beneficiary provided by the Client based on documents, data or information obtained from a reliable and independent source. Such actions of the Company also include a request to the Client to indicate the public sources where the information about the Beneficiary could be confirmed. The Client confirms the correctness of the data provided with its signature and seal (if it is required to have a seal according to the legislation regulating its activities).

8.4. If the Client is identified without its physical presence, the Client - a natural person or the representative of the Client - a legal entity must submit the data about the Beneficiary specified in the Clause 8.2 of the present Policy. The data provided by the Client is confirmed by using the electronic identification means issued by the European Union and operating according to electronic identification schemes with a high or sufficient level of security assurance, or using a qualified electronic signature with a qualified electronic signature certificate that complies with the requirements of Regulation (EU) 910/2014, or using the electronic means allowing live video transmission or by signing a written document.

8.5. In all cases, the Company must collect and provide the following data about the Beneficiary at the request of FCIS:

8.5.1. Beneficiary identification data;

8.5.2. Evidence of verification of the information provided by the Client in reliable and independent sources;

8.5.3. Data on the ownership and control structure of the Client (legal entity).

8.6. The Beneficiary must always be identified before the end of the Client identification procedure.

8.7. The Client must provide the information about the Beneficiaries in the form prescribed by the Company and presented as an Annex to the present Policy.

9. IDENTIFICATION OF THE POLITICALLY EXPOSED PERSONS

9.1. Before entering into a business relationship with the Client, the employees of the Company must take measures to determine whether the Client and the Beneficiary are Politically Exposed Persons. During the determination whether the Client and the Beneficiary are Politically Exposed Persons, the employees of the Company apply at least two of these measures:

9.1.1. Ask the Client to disclose whether it or the Beneficiary is a Politically Exposed Person in the completed questionnaire;

9.1.2. Verify whether their declaration of private interests is available on the website of the Chief Official Ethics Commission and, if so, whether the positions specified in the declaration are the Important Public Positions;

9.1.3. Verify the data provided by the Client about the Client and the Beneficiary in international databases that store and accumulate information about the Politically Exposed Persons.

9.2. After having determined that the Client or at least one of its Beneficiaries are considered Politically Exposed Persons, the employees of the Company apply an enhanced identification process in accordance with the procedure provided in Chapter 12 of the present Policy.

9.3. Where a Politically Exposed Person ceases to hold an Important Public Position, the employees of the Company must continue to take into account the risk posed by that person for a period of at least 12 months and apply appropriate measures adapted to the level of risk until it is determined that that person no longer poses a risk typical of Politically Exposed Persons.

10. IMPLEMENTATION OF INTERNATIONAL FINANCIAL SANCTIONS AND RESTRICTIVE MEASURES

10.1. Before entering into a business relationship with the Client, the employees of the Company must verify whether the Client or its Beneficiary is included in the list of persons subject to international financial sanctions or restrictive measures. Before entering into a business relationship with the Client, the employees of the Company verify whether the Clients or their Beneficiaries are not included in at least the following lists:

10.1.1. United Nations Security Council Consolidated List;

10.1.2. Consolidated list of financial sanctions of the European Union.

10.2. After the employees of the Company determine that the Client or Beneficiary is included in the lists specified in the Clause 10.1 of the present Policy, the business relations are not established with them. If during the business relations it is determined that the Client or Beneficiary is included in the lists specified in the Clause 10.1 of the present Policy, the employees of the Company:

10.2.1. Terminate the implementation or execution of the obligations arising before determination whether the Client or Beneficiary is included in the lists specified in the Clause 10.1 of the present Policy, or suspend their execution immediately;

10.2.2. Terminate the transaction concluded before determination whether the Client or Beneficiary is included in the lists specified in the Clause 10.1 of the present Policy, or suspend their execution unilaterally and immediately;

10.2.3. Inform FCIS about it within 3 hours;

10.2.4. Provide FCIS with all data required for the surveillance.

11. SIMPLIFIED IDENTIFICATION

11.1. The simplified identification of the Client is carried out in cases where the Client's total amount invested/intended to invest in the crowdfunding platform "Crowdpear" administered by the Company does not exceed 15,000 Euros during the calendar year and the other conditions provided in the Article 15 (1) (11) of the Law are met.

11.2. During the simplified identification of the Client, the Company:

11.2.1. Collects the following data:

11.2.1.1. From the Client – natural person: data specified in the Clauses 6.2.1-6.2.3 of the Policy;

11.2.1.2. From the Client – legal entity: data specified in the Clauses 6.3.1-6.3.3 of the Policy.

11.2.2. Ensures that the first payment of the Client is made from an account held at a credit, payment or electronic money institution, when the credit, payment or electronic money institution is registered in a European Union member state or a Third State that has established requirements equivalent to the requirements of the Law, and the competent authorities supervise the compliance with these requirements.

11.3. The Company does not apply the simplified identification if there are circumstances specified in Chapter 12 of the present Policy, when it is necessary to carry out an enhanced identification of the Client.

11.4. If, during the continuous monitoring of the Client's business relations, it is determined that the risk of money laundering and/or terrorist financing is no longer low, the Company must take the measures set out in the present Policy and determine and verify the identity of the Client and the Beneficiary.

12. ENHANCED IDENTIFICATION

12.1. The employees of the Company carry out an enhanced identification of the Client by applying the additional means of identification of the Client and Beneficiary in the following cases:

12.1.1. Where the transactions or business relations are conducted with Politically Exposed Persons;

12.1.2. Where the transactions or business relations are conducted with natural persons living in high-risk Third Countries identified by the European Commission or legal entities established there. After the risk assessment, the enhanced Client identification measures do not have to be applied to branches or subsidiaries of financial institutions or other obliged entities established in the European Union where they hold the majority of shares and which are located in high-risk Third Countries determined by the European Commission, if those branches or subsidiaries comply with the requirements set by the whole group and are equivalent to the requirements of the Law;

12.1.3. If the higher risk of money laundering and/or terrorist financing is determined according to the risk assessment and management procedures established by the Company;

12.1.4. In cases specified by the European supervisory authorities and the European Commission.

12.2. During the enhanced identification of the Client, the employees of the Company must:

12.2.1. Obtain the approval of the Responsible Person to establish or continue the business relations with such Clients when they become Politically Exposed Persons or are classified as a high-risk group for money laundering and/or terrorist financing;

12.2.2. Take appropriate measures to identify the source of assets and funds related to the business relationship or transaction. The employees of the Company use one or more of the following measures:

12.2.2.1. Ask the Client to provide the reliable documents confirming the origin of income or assets, such as an employment contract, service provision contract, sale and purchase contract, financial statement documents, and determine the maximum limit of financing transactions allowed for this person based on the submitted documents;

12.2.2.2. Verify the publicly available information that can confirm or deny the origin of the Client's income and/or assets;

12.2.2.3. Verify the publicly available registers that contain information about a person's financial situation.

12.3. If the enhanced identification is applied due to the fact that business relations are carried out with natural persons residing in high-risk Third Countries identified by the European Commission or legal entities (or their Beneficiaries) established there, the employees of the Company must:

12.3.1. Receive additional information about the Client and the Beneficiary;

12.3.2. Receive additional information about the intended nature of the business relationship;

12.3.3. Receive information about the source of funds and assets of the Client and the Beneficiary;

12.3.4. Receive information about the reasons for expected or completed transactions;

12.3.5. Obtain the consent of the Responsible Person to establish or continue the business relations with these Clients;

12.3.6. Carry out enhanced continuous monitoring of business relations with these Clients by increasing the number and terms of control measures and selecting the types of transactions requiring further investigation;

12.3.7. Ensure that the first payment of the Client is made from an account held at a credit institution, when the credit institution is registered in a European Union member state or a Third State that has established requirements equivalent to the requirements of the Law, and the competent authorities supervise the compliance with these requirements

12.4. After having applied an enhanced identification, the employees of the Company carry out an enhanced continuous monitoring of the business relations of these Clients.

12.5. The Company must pay special attention to any threat of money laundering and/or terrorist financing that may arise from any type of goods, products, other human labour results, use of services provided or transactions carried out, when the aim is to conceal the identity of the Client or Beneficiary (tending to anonymity), as well as for business relations or transactions with the Client not identified by its physical presence, and, if necessary, to take measures to prevent the assets from being used for money laundering and/or terrorist financing immediately.

13. MONITORING OF BUSINESS RELATIONS

13.1. After having established the business relations with the Clients, the Company carries out the regular or enhanced continuous monitoring of operations (transactions) and the business relations of these Clients:

13.1.1. The regular monitoring of operations (transactions) and business relationships is carried out for Clients identified using the regular client identification procedures provided for in the present Policy. In this case, the continuous monitoring of Client operations is carried out and, if there are no suspicions, the data provided by the Clients and their verification in independent sources are reviewed and updated periodically, but at least once a year;

13.1.2. The enhanced monitoring of operations (transactions) and business relationships is carried out for Clients identified using the enhanced client identification procedures provided for in the present Policy. In this case, the continuous monitoring of Client operations is carried out and, if there are no suspicions, the data provided by the Clients and their verification in independent sources are reviewed and updated periodically, but at least twice a year.

13.2. During the continuous monitoring (regular and enhanced) of the operations (transactions) and business relationships with the Clients, the Company in all cases:

13.2.1. Performs a review of identification data of the Clients, their representatives and Beneficiaries;

13.2.2. Performs the verification of transactions concluded during the business relations to ensure that the executed transactions comply with the Company's knowledge about the Client, its business, the nature of the risk and knowledge about the source of funds;

13.2.3. Takes immediate actions to prevent money laundering and/or terrorist financing.

14. IDENTIFICATION OF SUSPICIOUS TRANSACTIONS, THEIR SUSPENSION AND INFORMATION SUBMISSION TO FCIS

14.1. The Responsible Person must notify FCIS if the Company knows or suspects that assets of any value are directly or indirectly obtained from a criminal act or participation in such an act, as well as if it knows or suspects that these assets are intended for one, several terrorists or a terrorist organization support immediately, no later than within one business day from the occurrence of such knowledge or suspicion.

14.2. The Responsible Person notifies FCIS about:

14.2.1. The suspicious monetary operations and transaction carried out by the Client, including:

14.2.1.1. The cases where the employees of the Company know, receive information, suspect, or have sufficient reason to suspect that money laundering and/or terrorist financing has occurred or is being attempted;

14.2.1.2. The cases where the employees of the Company suspect or have sufficient reason to suspect that the Client's funds were obtained from a criminal act;

14.2.1.3. The cases where the employees of the Company suspect or have sufficient reason to suspect that transactions or activities are related to terrorist financing.

14.2.2. The Client's wish to pay for the services received in cash, if the amount of cash to be paid is equal to or exceeds 15,000 Euro or an equivalent amount in foreign currency.

14.3. The suspicious monetary operations and transactions specified in the Clause 14.2.1 of the present Policy are determined:

14.3.1. Based on the Criteria for Identifying Suspicious Monetary Operations or Transactions approved by the Order No. V-240 of the Director of the Financial Crimes Investigation Service;

14.3.2. By paying attention to such Client activities that may be related to money laundering and/or terrorist financing due to their nature;

14.3.3. During the identification of the Client and the Beneficiary and continuous monitoring of the Client's business relations, including the investigation of transactions concluded during such relations.

14.4. The Responsible Person informs FCIS about the Monetary Transactions of the Client specified in the Clause 14.2.1 of the present Policy, regardless of the amount of Monetary Transaction. The most important criteria are the suspiciousness of Monetary Transactions and/or activities. The Responsible Person must inform not only about the executed, but also about the suspicious operations or transactions that are intended to be executed.

14.5. The Responsible Person informs FCIS about the Monetary Transactions that do not meet any of the criteria for identifying the suspicious Monetary Transactions or operations, but the employee of the Company became suspicious of the Monetary Transaction and/or the Client's activity. The suspicion can be caused by various objective and subjective circumstances, for instance, the Client performs Monetary Transactions that are not characteristic of its activity, provides incorrect data about itself or the Monetary Transaction, avoids providing additional information (documents), etc. The employees of the Company are obliged to obtain sufficient information about the basis and objectives of the Monetary Transaction and the origin of the funds to be able to analyse the activities and/or operations and transactions carried out by the Client properly, and must submit their conclusions in writing.

14.6. In cases where it is determined that the Client has performed or is performing a suspicious Monetary Transaction or operation, regardless of the amount of the Monetary Transaction or operation, the Responsible Person must:

14.6.1. Suspend that Monetary Transaction or operation, except for cases where it is objectively impossible to do so due to the nature of the Monetary Transaction or operation, the method of its execution or other circumstances;

14.6.2. And inform FCIS about this transaction or operation no later than within 3 business hours (if the monetary transaction or operation was not suspended due to the nature of the Monetary Transaction or operation, the method of its execution or other circumstances – within 3 business hours from identification of a suspicious monetary transaction or operation).

14.7. If the Company receives information that the Client intends or will attempt to carry out a suspicious Monetary Transaction or operation, the Company suspends the actions necessary to carry out the intended Monetary Transaction or operation, but only after informing the FCIS about it and receiving its approval. If the mentioned actions are carried out, the suspicious Monetary Transaction or operation must be suspended.

14.8. After the Company receives an instruction from FCIS, the Responsible Person suspends these operations or transactions within 10 business days from the time indicated therein or the occurrence of specific circumstances.

14.9. The Responsible Person must resume the suspended monetary transactions of operation, if the Company is not obliged to carry out a temporary restriction of ownership rights in accordance with the procedure established by the Code of Criminal Procedure within 10 business days from the date of submission of the notification to the FCIS or the date of receipt of the FCIS instruction to the Company.

14.10. After having received a written instruction from FCIS do not suspend the suspicious Monetary Transactions or operations carried out by the Client, the Company does not obligatorily suspend these operations or transactions from the moment of receipt of the written notice or the moment indicated therein, and immediately resumes the suspended operations or transactions, if the suspension of a monetary transaction or operation may interfere with the investigation regarding the legalization of money or assets obtained through criminal means, terrorist financing and other criminal acts related to money laundering and/or terrorist financing.

14.11. During the execution of the obligation specified in the Clause 14.2, the Company follows the Procedure for Suspending Suspicious Monetary Transactions or Operations and Submitting Information About Suspicious Monetary Transactions or Operations to the Financial Crimes Investigation Service approved by the Minister of Interior of the Republic of Lithuanian additionally.

14.12. During the information submission to FCIS in cases specified in the Clause 14.2 of the present Policy, the information provided indicates the data confirming the identity of the Client, and if the Monetary Transaction is performed through a representative - the data confirming the identity of the representative, amount of the Monetary Transaction, currency of the Monetary Transaction, date of the Monetary Transaction, method of the Monetary Transaction and the entity in whose favour the Monetary Transaction was performed. This information is provided to the Financial Crimes Investigation Service immediately, no later than within 7 business days from the date of execution of the Monetary Transaction or conclusion of the transaction.

15. CLASSIFICATION OF CLIENTS INTO RISK GROUPS AND INFORMATION UPDATE

15.1. The Company classifies the Clients into the following groups:

15.1.1. posing a low threat of money laundering and/or terrorist financing;

15.1.2. posing a medium threat of money laundering and/or terrorist financing; and

15.1.3. posing a high threat of money laundering and/or terrorist financing.

15.2. The Clients of the Company are classified as Client groups posing a medium threat of money laundering and/or terrorist financing, except in cases where:

15.2.1. There are grounds for assigning them to the group of Clients posing a low threat of money laundering and/or terrorist financing or;

15.2.2. There are grounds for assigning them to the group of Clients posing a high threat of money laundering and/or terrorist financing.

15.3. The Clients of the Company are classified into risk groups by taking into account the criteria and procedure set out in the Annex to the present Policy.

16. LOG FILLING AND STORAGE PROCEDURE

16.1. In the course of its activities and in compliance with the requirements provided by the Law regarding the storage of information and documents, the Company maintains the registration logs. The logs are maintained electronically.

16.2. The Company maintains the following logs:

16.2.1. Suspicious Monetary Transactions or operations;

16.2.2. Notifications about the suspicious Monetary Transaction to FCIS;

16.2.3. Customers with whom the transactions or business relations have been terminated in circumstances related to breaches of the present Money Laundering and Terrorist Financing Prevention Policy.

16.3. The Company registers the following information in the registration logs:

16.3.1. Data confirming the identity of the Client and its representative (if the Monetary Transaction or operations is carried out through the representative) (natural person – name and surname, personal code (date of birth, in case of foreigner), citizenship; legal entity – name, legal form, seat address, code, if any);

16.3.2. Data about the Monetary Transaction or operation – the date of transaction, the description of the assets for which the transaction is concluded and its value (for instance, amount of money, the currency of a monetary transaction or operation, the market value of the assets);

16.3.3. Data about the person – recipient of the monetary funds (natural person – name and surname, personal code (date of birth, in case of foreigner), citizenship; legal entity – name, legal form, seat address, code, if any).

16.4. The data about the Beneficiary(-ies) is additionally recorded in the logs (name and surname, personal code (date of birth, in case of foreigner), citizenship) and indicates the criteria approved by the Financial Crimes Investigation Service, according to which it is recognized that the Client‘s Monetary Transaction or operation is considered suspicious, the transaction or operation meets.

16.5. The data is recorded in the registration log in chronological order, based on the documents confirming the Monetary Transaction or operation or other legally binding documents related to the execution of Monetary Transactions or the conclusion of transactions, immediately, but no later than within 3 business days after the execution of the Monetary Transaction or conclusion of the operation.

16.6. The Company ensures that the log data is protected from unauthorized destruction, alteration or use.

16.7. The registration data is stored in electronic media for 8 years from the date of the end of transactions or business relations with the Client. The Director of the Financial Crimes Investigation Service sets the Rules for managing the registration logs.

16.8. The data is stored for the following periods (except for cases where the longer storage periods are provided for in the Law on Crowdfunding of the Republic of Lithuania):

16.8.1. Copies of the documents identifying the Client, identity data of the Beneficiary, identity data of the payee, live video recording, other data obtained during the Client identification, invoice and/or contract documentation (original documents) must be stored for 8 years after the day of the end of transactions or business relations with the Client;

16.8.2. The correspondence of business relations with the Client must be stored in paper form or in electronic media (Client‘s file) for 5 years from the date of the end of transactions or business relations with the Client;

16.8.3. The documents and data confirming a Monetary Transaction or operation or other legally valid documents and data related to the execution of Monetary Transactions or the conclusion of operations must be stored for 8 years from the date of execution of the Monetary Transaction or conclusion of the operation.

16.8.4. The letters formalizing the investigation results specified in the present Policy are stored for 5 years in paper form or in electronic media (Client‘s file).

16.8.5. The storage periods can be additionally extended for a maximum of 2 years, in case of a reasoned instruction of the competent authority.

16.9. The data provided in the Clause 16.8 of the Policy must be stored so that it is possible:

16.9.1. To recover the specific Monetary Transactions or operations;

16.9.2. To present them and the information contained in them to the Financial Crime Investigation Service or other competent authorities, if necessary.

17. FUNCTIONS AND RESPONSIBILITIES OF THE RESPONSIBLE PERSON

17.1. The decision of the Manager of the Company appoints a Responsible Person for the prevention of money laundering and terrorism, who carries out the prevention measures of money laundering and/or terrorist financing provided for in the Policy. If the Manager of the Company does not appoint a Responsible Person or the Responsible Person is unable to perform his/her functions, the Responsible Person is deemed to be the Manager of the Company.

17.2. The functions of the Responsible Person include:

17.2.1. Log management and assurance of the data security;

17.2.2. Money laundering and terrorist financing risk assessment and management in all Company activities;

17.2.3. Suspension of suspicious monetary transactions;

17.2.4. Implementation, review and update of money laundering and terrorist financing prevention measures;

17.2.5. Cooperation and communication with FCIS and other supervisory authorities in matters related to the prevention of money laundering and/or terrorist financing;

17.2.6. Familiarisation of the Company's employees with the present Policy;

17.2.7. Organization of periodic trainings on the prevention of money laundering and/or terrorist financing for the Company's employees.

17.3. Prior to the appointment of a Responsible Person, the Manager of the Company assesses his/her competence, work experience and qualifications in the field of money laundering and terrorist financing, level and nature of education, qualification improvement, nature and duration of professional activity or work experience, as well as other factors that may affect the competence of the person. The Manager of the Company ensures the appropriate separation of functions performed by the Responsible Person to avoid the conflicts of interest that increase or may increase the risk of money laundering and terrorist financing.

17.4. After having appointed a Responsible Person, the Company must inform FCIS about the appointment of such a person immediately, but no later than within 7 business days.

17.5. The Responsible Person is entitled to receive and familiarize himself/herself with all the information necessary to perform his/her functions, including the access to all information related to the Clients, their representatives, Beneficiaries and to information about all Monetary Transactions carried out by the Company and the Company's Clients.

17.6. The Responsible Person ensures that upon receipt of a FCIS request, the requested information is provided immediately, but no later than within 14 business days of receipt of the request (if the Law sets the shorter deadlines for submitting information to FCIS, such information must be submitted within the shorter deadlines)

17.7. The Responsible Person will ensure that the Policy and other measures of the Company for the prevention of money laundering and terrorist financing are reviewed at least once a year and updated if necessary.

17.8. The Responsible Person submits a report on the implementation of money laundering and terrorist financing measures to the Manager of the Company periodically, but at least once a year, with the following information:

17.8.1. Money laundering and terrorist financing risk management, including:

17.8.1.1. The Company's risk of money laundering and terrorist financing and changes in its level;

17.8.1.2. The implemented risk management measures of money laundering and terrorist financing;

17.8.1.3. The proposals for changing the measures necessary to effectively manage (reduce) the risk of money laundering and terrorist financing;

17.8.1.4. The information on violations identified during the implementation of internal control procedures and policies in the field of money laundering and terrorist financing prevention;

17.8.1.5. The reports how the Company fulfils the requirements and obligations related to the prevention of money laundering and terrorist financing.

17.9. If the employees of the Company suspect that a Monetary Transaction may be suspicious or discover other possible signs of money laundering and/or terrorist financing, they must immediately inform the Responsible Person.

18. FINAL PROVISIONS

18.1. The Manager of the Company approves the present Policy. The present Policy can be amended, changed or supplemented only by the decision of the Manager of the Company. The Policy or its amendments enter into force on the date of the decision of the Manager of the Company, except for those cases where a different effective date is provided for in the Manager's decision.

18.2. The Responsible Person must familiarise with the present Policy and ensure that all employees of the Company are familiarized with the present Policy by signing.