**Policy of counteracting** **money laundering and situations that generate**

**a conflict of interest in force**

**at the "Konflikt" Foundation with its registered office in Warsaw**

**Table of contents:**

**1. Glossary.**

**2. General provisions.**

**3. Notification to the Inspector General of circumstances that may indicate a suspicion of money laundering or financing of terrorism.**

**4. Assessment of risk related to money laundering and financing of terrorism.**

**5. Applying financial security measures to Clients.**

**6. Applying increased financial security measures.**

**7. Determining the date and method of storing documents.**

**8. Policy of informing about a conflict of interest.**

**9. Zero tolerance policy for abuses.**

**10. Liability for breach of terms.**

**11. Responsibilities of the Management Board.**

**1. Glossary.**

Whenever this document refers to:

1) **Document** – it should be understood as this Policy of Counteracting Money Laundering and Situations That Generate a Conflict of Interest.

2) **Entity** – it should be understood as the “Konflikt" Foundation with its registered office in Warsaw (02-577), Aleja Niepodległości 118/89, entered into the Register of Associations, other social and professional organisations, foundations and public health care institutions and into the Register of Entrepreneurs of the National Register Court conducted by the District Court for the Capital City of Warsaw in Warsaw, 13th Commercial Division of the National Court Register under KRS number: 0000635116, NIP: 1132917279, REGON: 365350266.

3) **Entity’s Staff** – it should be understood as any natural person providing work in the Entity, regardless of the type of employment contract concluded and the position held, including a person cooperating with the Entity on the basis of a civil law contract.

4) **Management Board** – it should be understood as the body authorised to represent the Entity in accordance with the National Court Register.

5) **Client** – it should be understood as all entities that are related to the Entity in a business manner, i.e.: associates, consultants, suppliers, contractors and all entities in relations with the Entity to which funds are transferred;

6) **Inspector General** – it should be understood as a government administration authority competent in matters of counteracting money laundering and financing of terrorism;

7) **Business Relations** – it should be understood as the relations of the Entity with the Client related to the activity of the Entity, which at the time of their establishment show the feature of durability;

8) **Transaction** – it should be understood as a legal or factual act on the basis of which the transfer of ownership or possession of property values ​​is made, or a legal or factual act made for the purpose of transferring ownership or possession of property values;

9) **Occasional Transaction** – it should be understood as a transaction that is not carried out as part of business relations.

2. **General provisions.**

1. The Management Board is responsible for compliance with the provisions of the Act of 1 March 2018 on counteracting money laundering and financing of terrorism (Journal of Laws 2022.593, i.e. of 2022.03.15), hereinafter referred to as: the “Act”.

2. The person responsible for implementing the obligations set out in the Act is Jarmiła Rybicka, Chair of the Management Board of the Foundation.

3. Each member of the Entity's Staff is obliged to familiarise themselves with the provisions of this Document and to sign a declaration on familiarising oneself with the Document, which is attached as Appendix 1 to this Document.

3. **Notification to the Inspector General of circumstances that may indicate a suspicion of money laundering or financing of terrorism.**

1. The Management Board shall immediately notify the Inspector General, by means of electronic communication, of the case of **justified** suspicion that a specific Transaction or specific assets may be related to money laundering or financing of terrorism.

2. The Management Board shall immediately notify the competent prosecutor of a **justified** suspicion that the assets being the subject of the Transaction or accumulated in the account originate from a crime other than the crime of money laundering or financing of terrorism or from a tax offence or are related to a crime other than the crime of money laundering or financing of terrorism or a tax crime.

3. The Management Board shall immediately notify the Inspector General, by means of electronic communication, about the Transaction referred to in art. 86 section 1 of the Act (suspicious transaction), if it was impossible to submit the notification before it was carried out.

4. **Assessment of risk related to money laundering and financing of terrorism.**

1. The Entity identifies and assesses money laundering and financing of terrorism risks related to its activities.

2. When performing the analysis to determine the amount of risk, the Entity takes into account in particular the following criteria:

1) economic – consisting in assessing the Transaction with the Client in terms of the purpose of their business activity,

2) geographical – consisting in making Transactions unjustified by the nature of business activity concluded with entities from countries where there is a high risk of money laundering and financing of terrorism,

3) objective – consisting in the Client's high-risk business activity from the point of view of susceptibility to money laundering and financing of terrorism.

3. The risk assessment referred to in section 1 above, the Entity prepares in paper or electronic form and, if necessary, but not less frequently than every 2 years, updates it, in particular in connection with changes to the above-mentioned criteria.

5. **Applying financial security measures to Clients.**

1. The Entity applies financial security measures to its Clients.

2. The Entity applies financial security measures to the extent proportional to the identified risk of money laundering and financing of terrorism.

3. Financial security measures include:

1) identification of the Client and verification of their identity, and if a designated person acts on behalf of the Client, the identity of the person authorised to act on behalf of the Client and the authorisation to act on behalf of the Client are subject to identification. The Client's identity is verified before establishing business relations or conducting an Occasional Transaction;

2) assessing the business relations and, where appropriate, obtaining information on its purpose and intended nature;

3) ongoing monitoring of the Client's business relations, including:

a) analysis of Transactions carried out as part of business relations in order to ensure that these Transactions are consistent with the Entity's knowledge of the Client, the type and scope of the Client’s business and the risk of money laundering and financing of terrorism associated with this Client,

b) examination of the source of origin of property values ​​at the disposal of the Client – in cases justified by circumstances,

c) ensuring that the documents, data or information regarding business relations are kept up-to-date.

4. The Entity applies financial security measures in the case of:

1) establishing business relations;

2) conducting an Occasional Transaction:

a) equivalent of PLN 30,000 or more, regardless of whether the Transaction is carried out as a single operation or several operations that seem to be related, or

b) which is a transfer of funds for the amount exceeding the equivalent of PLN 20,000,

c) using a virtual currency with the equivalent of PLN 20,000 or more – in the case of the obligated institutions referred to in Art. 2 sec. 1 point 12 of the Act;

3) carrying out an occasional cash Transaction equivalent of PLN 5,000 or more, regardless of whether the Transaction is carried out as a single operation or several operations that seem to be related;

4) suspicion of money laundering or financing of terrorism;

5) doubts as to the veracity or completeness of the Customer's identification data obtained thus far.

5. The Entity applies financial security measures also in relation to Clients with whom it maintains business relations, taking into account the identified risk of money laundering and financing of terrorism, in particular when:

1) there has been a change in the previously established nature or circumstances of the business relations;

2) there has been a change in the previously agreed data concerning the Client.

6. The Entity, taking into account the identified risk of money laundering and financing of terrorism, may refrain from applying security measures in relation to electronic money within the meaning of the Act of 19 August 2011 on payment services, provided that the conditions referred to in Art. 38 of the Act are met.

6. **Applying increased financial security measures.**

1. The Entity applies increased financial security measures in cases of higher risk of money laundering or financing of terrorism.

2. The Entity also applies increased financial security measures in cases of business relations or Transactions related to a high-risk third country identified by the European Commission in a delegated act adopted pursuant to Art. 9 of Directive 2015/849. Due to the high risk, the Entity undertakes the following actions:

1) obtains additional information about:

a) the Client,

b) the intended nature of the business relations;

2) obtains information about the source of the Client's assets and the source of origin of the assets at the Client's disposal as part of business relations or Transactions;

3) obtains information about the reasons and circumstances of intended or carried out Transactions;

4) obtains the approval of the Management Board for the establishment or continuation of business relations;

5) intensifies the application of the financial security measure referred to in Art. 34 sec. 1 point 4 of the Act, by increasing the number and frequency of monitoring business relations and increasing the number of Transactions selected for further analysis.

3. With regard to politically exposed Clients, the Entity:

1) assesses the risk by checking, on the basis of generally available information, including information contained on the Internet, whether the Client is a politically exposed person,

2) takes possible measures to determine the source of the assets introduced to the market,

3) conducts constant control of the Transactions carried out.

4. The Entity conducts an ongoing analysis of the Transactions carried out in relation to Clients for whom it applies increased financial security measures.

5. In the event of disclosure of complex Transactions or those involving high amounts, which are not justified by the circumstances of the Transaction, or conducted in an unusual manner, or which seem to have no legal or business justification, the Entity takes steps to clarify the circumstances in which these Transactions were carried out, and, in the case of Transactions carried out as part of business relations, it increases the application of the financial security measure referred to in art. 34 sec. 1 point 4 of the Act, in relation to the business relations under which these Transactions were carried out.

7. **Determining the date and method of storing documents.**

1. The Entity stores for a period of 5 years, counting from the date of termination of business relations with the Client or from the date of conducting an Occasional Transaction,:

1) copies of documents and information obtained as a result of applying financial security measures, including information obtained by means of electronic identification and trust services enabling electronic identification within the meaning of Regulation 910/2014;

2) evidence confirming the Transactions carried out and Transaction records, including original documents or copies of documents necessary to identify the transaction.

2. The Entity stores the results of the analyses referred to in Art. 34 sec. 3 of the Act, for a period of 5 years from the date of their implementation.

3. Documents are stored in a specially designated place, inaccessible to unauthorised persons.

8. **Policy of informing about a conflict of interest.**

1. A conflict of interest is a situation in which a member of the Entity's Staff, as a result of external or internal circumstances or their own actions, is obliged to achieve goals that cannot be achieved simultaneously with taking into account the broadly understood interest of the Entity. This applies to situations where, acting for their own benefit or for the benefit of another person or entity to whom they have obligations, a member of the Entity's Staff acts at the same time against the interest of the Entity to which they should also be loyal.

2. When handling matters, the Entity's Staff is obliged to assess the possibility of a conflict of interest on an ongoing basis – if they consider that a conflict of interest may arise, they are obliged to immediately notify the Management Board of this fact.

3. In the event of confirming the possibility of a conflict of interest, the Management Board excludes a member of the Entity's Staff from handling the case.

8. **Zero tolerance policy for abuses.**

1. The Entity's Staff is obliged to inform the Management Board of any irregularities and abuses that may constitute a violation of the law.

2. In a situation where a Client, towards whom official activities are performed, takes actions indicating an intention to give a financial or personal benefit to a member of the Entity's Staff, or to make a promise of such an advantage, the Entity's Staff:

1) informs the Client that their behaviour may meet the criteria of a crime specified in the Penal Code;

2) without leaving the scene of the event, informs the Management Board about the situation by phone or electronically;

3) draws up a memo documenting the course of the event.

3. In the event that the Entity's Staff is in possession of information or has a reasonable belief about the possibility of irregularities or abuse, they are obliged to provide the information to the Management Board in a documented form.

4. An incident report should:

1) be in writing;

2) include the date of the event;

3) contain a detailed description of the event/situation;

4) indicate the name of the entity or person who participated in the event.

5. The reporting person, if they are able to obtain evidence confirming the event, should secure it or attach it to the report.

9. **Liability for breach of terms.**

1. The Entity's Staff bears employee liability for violation of the provisions, including the principles set out in this Document.

2. Members of the Entity's Staff should disseminate knowledge of this Document to other members of the Entity's Staff.

10. **Responsibilities of the Management Board.**

The Management Board is obliged to:

1) familiarise all members of the Entity's Staff with the content of this Document within 7 (say: seven) days from the date of entry into force of this Document;

2) consider complaints and other notifications regarding unethical behaviour of members of the Entity's Staff.

Appendix No. 1 – Declaration on familiarisation of a member of the Entity's Staff with the Policy of

counteracting money laundering and situations that generate a conflict of interest

Warsaw, on ………………..

**DECLARATION**

I, the undersigned ………………………………, hereby declare that I have read and will comply with the provisions of the Policy of counteracting money laundering and situations that generate a conflict of interest applicable at the “Konflikt” Foundation based in Warsaw.

At the same time, I declare that I am aware of liability in the event of violation of the provisions set out in the above-mentioned document and criminal liability under the generally applicable law.

………………………………………..

Name and surname