Last Update: November 01, 2022

AML Policy - Damir Invest OÜ

Damir Invest OÜ ("**Damir**" or "**Company**") has no tolerance for money laundering, the financing of terrorism or any other form of illicit activity, and is committed to implementing policies, procedures and controls shaped by the best industry practices and the most effective anti-money laundering standards applied in the Republic of Estonia and worldwide. These rules apply to, without exception, all employees of the Company, its Board members, officers, contractors, and consultants.

The purpose of this document is to provide the Company's partners, clients, vendors, contractors, employees, regulators, law enforcement and other concerned stakeholders with a high-level overview of the Company's AML/CTF compliance regime elements and procedures. By no means this document shall not be read as an entire set of all policies, procedures and controls in place implemented by the Company for prevention of money laundering, financing of terrorism and other forms of illicit activity.

This document and all underlying policies, processes and procedures are prepared in line with provisions, requirements and recommendations of:

1. Money Laundering and Terrorist Financing Prevention Act of Estonia, as amended from time to time ("**Act**");
2. International Sanctions Act of Estonia as amended from time to time; and
3. FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Assets Service Providers.

The Company operates from, and under the laws of the Republic of Estonia. Estonia was among the first countries in the world who introduced Anti-money laundering ("**AML**") and countering the financing of terrorism ("**CTF**") requirements for businesses engaged in exchange of virtual currency for fiat currency and virtual currency custody back in 2017. As a result, each entity rendering named services from or within the territory of Estonia must apply for authorization to the Financial Intelligence Unit of Estonia ("**FIUE**").

Damir Invest OÜ is authorized to provide services of exchanging virtual currency against fiat currency and virtual currency wallet service (License No.: FVT000154) by the FIUE. The licenses can be validated on the official website of the Ministry of Economic Affairs and Communications of Estonia.

As a regulated business, Damir is required to comply with the Money Laundering and Terrorist Financing Prevention Act and International Sanctions Act, which require Damir to identify and verify its clients' identities, conduct ongoing monitoring of their activity, including transaction monitoring, maintain records of clients' activity and related documents for at least five years and report certain transactions to authorities.

The Company understands *money laundering* as:

1. the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
2. the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

3. the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;
4. participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in points 1, 2 and 3.

Terrorist financing means providing funds for terrorist activity. From legal standpoint it means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA. Terrorist activity has as its main objective to intimidate a population or compel a government to do something. This is done by intentionally killing, seriously harming or endangering a person, causing substantial property damage that is likely to seriously harm people or by seriously interfering with or disrupting essential services, facilities or systems.

Risk-Based Approach and Risk Assessment

Damir will perform a risk-based due diligence and collect information and documentation on each prospective client in order to assess the risk profile associated. The Company's employees will exercise care, due diligence and good judgement in determining the overall character and nature of all clients. Damir conducts its business in accordance with the highest ethical standards and will not enter into business relationships with individuals or entities that may adversely affect Company's reputation and compromise virtual currency industry.

For the purpose of identification, assessment and analysis of risks of money laundering and terrorist financing related to its activities, the Company prepares a risk assessment, taking account of the following categories:

1. Customer risk;
2. Geographical risk;
3. Product risk; and
4. Delivery channel risk.

After the risk assessed and attributed to a particular customer, depending on degree of risk, it should be revised periodically upon knowledge of the customer and its activity.

Compliance Officer

The management board of the Company shall appoint a Compliance Officer, who acts as a contact person of the FIUE and performs AML/CTF duties and obligations of the Company. A Compliance Officer reports directly to the management board and has the competence, means and access to relevant information across all the structural units of the Company.

Only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties listed below may be appointed as a Compliance Officer. The appointment of a Compliance Officer is coordinated with the FIUE.

The duties of a Compliance Officer include, inter alia:

1. organisation of the collection and analysis of information referring to unusual transactions or transactions or circumstances suspected of money laundering or terrorist financing, which have become evident in the activities of the Company;

2. reporting to the FIUE in the event of suspicion of money laundering or terrorist financing;
3. periodic submission of written statements on compliance with the requirements arising from the Act to the management board of the Company;
4. performance of other duties and obligations related to compliance with the requirements of the Act.

Rules of Procedure and Internal Control Rules

The Company has developed and implemented rules of procedure that allow for effective mitigation and management of risks relating to money laundering and terrorist financing, which are identified in the risk assessment performed in accordance with the Company's risk-based approach described above.

Each employee of the Company should strictly adhere to rules of procedure set forth herein.

The rules of procedure consist of the following:

1. a procedure for the application of due diligence measures regarding a customer, including a procedure for the application of simplified and enhanced due diligence measures;
2. a model for identification and management of risks relating to a customer and its activities and the determination of the customer's risk profile;
3. the methodology and instructions where the Company has a suspicion of money laundering and terrorist financing or an unusual transaction or circumstance is involved as well as instructions for performing the reporting obligation;
4. the procedure for data retention and making data available;
5. instructions for effectively identifying whether a person is a politically exposed person or a local politically exposed person subject to international sanctions.

The Company applies the following due diligence measures:

1. identification of a customer and verification of the submitted information based on information obtained from a reliable and independent source, including using means of electronic identification and of trust services for electronic transactions;
2. identification of the beneficial owner and, for the purpose of verifying their identity, taking measures to the extent that allows the Company to make certain that it knows who the beneficial owner is, and understands the ownership and control structure of the customer;
3. understanding of business relationships, and, where relevant, gathering information thereon;
4. gathering information on whether a person is a politically exposed person, their family member or a person known to be close associate;
5. monitoring of a business relationship.

Simplified Due Diligence

The Company may apply simplified due diligence ("**SDD**") measures where a risk assessment prepared on the basis of these rules of procedure identifies that, in the case of the economic or professional activity, field or circumstances, the risk of money laundering or terrorist financing is lower than usual.

Before the application of SDD measures to a customer, an employee of the Company establishes that the business relationship, transaction or act is of a lower risk and the Company attributes to the transaction, act or customer a lower degree of risk.

The application of SDD measures is permitted to the extent that the Company ensures sufficient monitoring of transactions, acts and business relationships, so that it would be possible to identify unusual transactions and allow for notifying of suspicious transactions in accordance with these rules of procedure.

Enhanced Due Diligence

The Company applies enhanced due diligence ("**EDD**") measures in order to adequately manage and mitigate a higher-than-usual risk of money laundering and terrorist financing.

EDD measures are applied always when:

1. upon identification of a person or verification of submitted information, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
2. the customer is a politically exposed person, except for a local politically exposed person, their family member or a close associate;
3. the customer is from a high-risk third country or their place of residence or seat in a high-risk third country;
4. the customer is from such country or territory that, according to credible sources such as mutual evaluations, reports or published follow-up reports, has not established effective AML/CTF systems that are in accordance with the recommendations of the Financial Action Task Force, or that is considered a low tax rate territory.
5. The Company applies EDD measures also where a risk assessment prepared on the basis of these rules identifies that, in the case of the economic or professional activity, field or factors, the risk of money laundering or terrorist financing is higher than usual.

PEP Definition and Screening

Politically Exposed Persons ("**PEP**") (as well as their families and persons known to be close associates, as described below) are required to be subject to enhanced scrutiny by reporting entities. This is because international standards issued by the Financial Action Task Force recognize that a PEP may be in a position to abuse their public office for private gain and a PEP may use the financial system to launder the proceeds of this abuse of office.

PEP means a natural person who is or who has been entrusted with prominent public functions including:

1. head of State;
2. head of government;
3. minister and deputy or assistant minister;
4. a member of parliament or of a similar legislative body;
5. a member of a governing body of a political party;
6. a member of a supreme court;
7. a member of a court of auditors or of the board of a central bank;
8. an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces;
9. a member of an administrative, management or supervisory body of a State-owned enterprise;
10. a director, deputy director and member of the board or equivalent function of an international organisation,

PEPs do not include middle-ranking or more junior officials.

Family member of a PEP means the spouse, or a person considered to be equivalent to a spouse, of a PEP or local PEP; a child and their spouse, or a person considered to be equivalent to a spouse, of a PEP or local PEP; a parent of a PEP or local PEP.

Person known to be close associate of a PEP means a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a PEP or a local PEP; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a PEP or local PEP.

Sanctions Screening

Dealing with persons against which imposed international sanctions poses a great risk to the Company, its directors, officers and owners.

The Company will perform sanction screening of its customers on the same matching rules, as for PEP screening.

The Company will perform screening, at minimum, against the following sanctions lists:

1. UN Sanctions;
2. EU Sanctions;
3. Sanctions administered by the Office of Financial Sanctions Implementation ("OFSI-UK")
4. Sanctions administered by the Office of Foreign Assets Control ("OFAC-US");
5. Sanctions imposed under the International Sanction Act.

All matches (true hits) will be escalated to a Compliance Officer for further action and processing.

Suspicious Activity Monitoring and Reporting

Where the Company identifies an activity or facts whose characteristics refer to the use of criminal proceeds or terrorist financing or other criminal offences or an attempt thereof or with regard to which the Company suspects or knows that it constitutes money laundering or terrorist financing or the commission of another criminal offence, a Compliance Officer of the Company must report it to the FIUE immediately, but not later than within two working days after identifying the activity or facts or after getting the suspicion.

The Company and all its employees, officers and directors are prohibited to inform a person, its beneficial owner, representative or third party about a report submitted on them to the FIUE, an intention to submit such a report as well as about the commencement of criminal proceedings.

Data Retention

The Company must retain the documents and information which served for identification and verification of clients, no less than five years after termination of the business relationship.

The Company implements necessary rules for protection of personal data upon application of the requirements arising from its obligations hereunder.

The Company is allowed to process personal data gathered upon implementation of these rules only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

Training

The Compliance Officer shall ensure that Company's employees are fully aware of their legal obligations under the AML/CTF regime, by introducing a complete employees' education and training program.

The timing and content of the training provided is determined according to the needs of the Company. The frequency of the training can vary depending on to the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the business model. The training program aims at educating the Company's employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose.

Cooperation and Exchange of Information

The Company cooperates with supervisory and law enforcement authorities in preventing money laundering and terrorist financing, thereby communicating information available to the Company and replying to queries within a reasonable time, following the duties, obligations and restrictions arising from legislation. For any relevant requests please contact us at aml@damirinvest.ee. Please note that in case you represent the law enforcement agency outside of the European Union, procedure under the Mutual Legal Assistance Treaty (MLAT) may apply.