DISCIPLINA OÜ

RULES OF INTERNAL CONTROL REGARDING PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM

1. General provisions

1.1 The current AML policy has been developed in accordance with the applicable legislation of the Republic of Estonia.

1.2 The AML policy is a set of internal rules and regulations that is used by the Company in order to check and reveal documentation and information regarding its operation that is under obligatory control, and other operations with money or property that may be in any way connected to money legalisation (money laundering) or finance of terrorism, and the provision of such information to the state authorities.

1.3 The AML policy is a document that:

1.3.1 Regulates the organisation of activity regarding the prevention of legalisation of illegally obtained funds (money laundering) and the financing of terrorism;

1.3.2 Sets the obligations and obligatory procedures for the employees regarding internal control;

1.3.3 Sets the terms for the fulfilment of obligations by the employees and sets the authorized control persons.

1.4 The AML policy contains further programs:

1.4.1 A program for the overview of internal control methods;

1.4.2 A program for the implementation of internal control methods;

1.4.3 Client and persons associated with client’s identification program;

1.4.4 A risk analysis program;

1.4.5 A program for the regulation of commercial relations with clients;

1.4.6 A program for the regulation obligatory actions in case there are suspicions of money laundering;

1.4.7 A correspondence exchange program;

1.4.8 An information documentation program;

1.4.9 A transaction refusal program;

1.4.10 An employee preparation program;

1.4.11 An internal control program;

1.4.12 A document maintenance program regarding documentation that was obtained during the execution of the internal control program.

1.5 The company is providing the cryptocurrency and cryptocurrency wallet services.

1.6 The person responsible for the accurate implementation of the present policy is named by the company management board in accordance with the articles of association and applicable legislation.

2. Organizational basis for the control methods

2.1 The person responsible for the implementation of the provisions in the present document is appointed by the written order of the management board of the company.

2.2 In order to adequately implement the current policy, considering the volume of clients and associated risk levels, the company has formed a separate group, including a member of the board, the head accountant and the head of the legal department.

2.3 All subsidiaries and structural parts are accountable before the authorized group in the field of suspicious transactions. All matters regarding initial client identification are handled by the corresponding structural parts of the company.

2.4 A company official is named as the contact person between Disciplina OÜ and the Financial inspection of Estonia. The contact person must have the required knowledge and skills to carry out his obligation and the present policy. The contact person shall only be accountable before a member of the board and will perform the following tasks:

- An analysis of the performed or planned transaction regarding their possible connection to money laundering or finance of terrorism;
- Presentation to the financial inspection of any data regarding clients, their associated persons, and transactions, which may be connected to illegal activity;
- Presentation of reports regarding the fulfilment of this policy;
- Fulfilment of other obligations as set out in the “Money laundering and terrorism finance prevention act”.

3. Implementation of control methods

3.1 Control methods are used in the following areas:

- during the initiation of a commercial relationship with the client and during their activity;
- in any case when the sum of the transaction exceeds 6400 EUR or an equivalent in any other currency;
- if there is any doubt that the provided data is accurate;
- if the planned transaction is needlessly complex;

- if there is any reason to suspect that the transaction is connected with money laundering or finance of terrorism or any other form of illegal activity or is considered a high-risk transaction in accordance with the risk evaluation procedure set out in the current policy.

3.2 Additional control methods are implemented in the event that the Client changes the conditions of the transaction, increasing the risk level:

- If the transaction serves no rational purpose;
- If the transaction is financially irrational;
- If the same type of transaction is repeated multiple times over a short period;
- Should the client refuse to provide information without giving a reason for the refusal or should the client express unusual concern with the matters of confidentiality;
- Should the Client decide to alter the transaction in a manner that is not the usual practice of the organisation;
- Should the client express unreasonable hurry to carry out the transaction;
- Should the client implement changes into the transaction conditions shortly before it is performed;
- Should the client prove impossible to contact;
- Should there be any information that the data provided by the client is false or inaccurate;
- In case of absence of any association between the activities of the Client and the planned transaction;
- Should the planned transaction be needlessly complicated and lacking any legal purpose.

3.3 Additional methods for the control of a suspicious transaction:

- Receipt from the client with the necessary explanation and confirmation that clarify the purpose of the transaction;
- Implementation of increased monitoring in accordance with the present policy regarding all the transactions of the Client in order to confirm if they are in any way connected to money laundering or the finance of terrorism.

4. Client and their associated persons identification program

4.1 The initial identification of the client is made on the basis of the provided client identification document.

4.1.1 Regarding the physical persons the following is confirmed:

- Name;
- Surname;
- Patronymic (when applicable to national custom);
- Citizenship;
- Date of birth, personal ID number;
- ID document data;
- Place of residence;
- Personal tax number (if applicable);
- Occupation;
- Reason for initiated commercial relations;
- Contact information – phone number, email address.

4.1.2 During identification, the documents are checked for accuracy of the information provided and the following is confirmed:

- Whether the identification document is legally valid;
- Is the photo on it accurate;
- Whether the personal ID code corresponds to the client's gender and age.

Should there be any doubt regarding the document, the state authorities that issued the document may be contacted in order to obtain the necessary confirmation.

4.1.3 Should the Client present an ID, a copy is made, the quality of which allows to review the data contained in the document.

4.1.4 When the identity of a physical person is confirmed it is also confirmed whether he is a state official;

A state official is a person who has a state appointed position in any country of the European Union or any other country or who holds a position in an International organisation. Further data regarding the state officials to be gathered:

- List of the closest associates and relatives (if such information is publically available);
- Confirmation of the property and sources of income that are meant to be used in the transaction;
- Preparation of an inquiry to the proper database;
- Preparation of an inquiry to the state supervision institutions;
- A decision regarding the start of the commercial relationship with the state official is made by a person named in accordance with provision 2.1 of this policy.

4.1.5 Only official sources may be used to check the provided information, such as state registries or foreign representatives. Other sources may be used if there is no doubt regarding their accuracy and competence.

4.1.6 Trustworthy Client recommendation does not replace the proper review of information.

4.1.7 Identification of a physical person that acts as a representative is made in accordance with the provisions of this policy.

4.1.8 Identification of a physical person is not a one-time procedure. The information regarding the physical person should be checked constantly and updated when necessary.

4.1.9 Should there be any doubt, the actual beneficiary must be revealed – a person that actually controls the legal person and receives profit from it.

4.2 The following information must be obtained during the registration of a legal person:

4.2.1 Regarding the legal persons the following information is gathered:

- Name of the legal entity;
- Registration number;
- Legal address and the address of principal activity;
- Corporate form;
- Full information regarding legal representatives;

- Beneficiaries.

4.2.2 The review of information is made by the use of public registries and databases or by sending inquiries to the state authorities. Certificate from a registry may be replaced by an authorised access to the registry.

4.2.3 All documents issued by foreign state authorities must be legalised or have an apostille, except the documents from Latvia, Lithuania, Poland, Russia, or Ukraine. The present provision may be amended if Estonia signs and ratifies an international agreement with other states that will make the apostille unnecessary.

4.2.4 The control of the legal entity management board or another similar control organ must also be carried out regarding their connection to state officials, also regarding beneficiaries and their representatives. Should the information provided by the Client not be trustworthy enough, the information may be reviewed by the means of an inquiry to state officials or international organisations.

4.2.5 All the provided information is gathered and carefully studied to reveal whether the company has any subsidiaries, representatives or is in any way connected to countries that do not cooperate in the field of international opposition to money laundering and finance of terrorism, or if those states are considered to be low tax jurisdictions.

4.2.6 If the legal entity is an international organisation, then its field of activity must be confirmed by the provisions of documentation regarding activities in Estonia. The information in the documents must be checked.

4.3 If the legal entity acts as a representative of another entity, then the information of that other entity must also be gathered in accordance with this policy.

4.3.1 Only an authorised legal representative may register a legal entity on the website of Disciplina OÜ. The authorised representative must provide sufficient documentation proving his authority to represent the legal person. Should the provided documents fail to provide the required information or if there is any doubt regarding their accuracy, no commercial relationship may be initiated and the account may be blocked. The document proving the authority must contain further information:

- Scope of rights;
- Date the authority was granted and for what period;
- Reason the authority was granted.

4.4 Any transaction with the legal person requires the registration of the current beneficiary.

4.4.1 Should a person have more than one beneficiary, then all other beneficiaries must also be registered.

4.4.2 Should it prove impossible to clarify the beneficiaries of the company, all owners of the company must be confirmed and sufficient explanation must be provided by the Client.

4.4.3 Special care should be taken when confirming the actual beneficiary if the planned transaction may in any way be connected to the increase of the risk due to the field of activity of the legal person, state of registration, type of provided services and nature of the transaction, and also if the legal person is registered or connected to a low tax jurisdiction.

4.5 A non-resident legal person must abide by the same identification process outlined above. Disciplina OÜ has the right to deny any transaction if the legal person is a resident of a country whose legislation violates the provisions of this AML policy.

4.6 Should the risk of the transaction be considered low or should there be reasons to consider the risk of commercial relations low, a simplified control method of client identification may be used, by checking the data through the publically available databases that can be considered trustworthy. Aside from the low risk level that was given under the risk analysis following the provisions of part 5 of this Document, additional reasons to consider the transaction to be low risk are the following:

- the Client is an Estonian public legal person;
- The Client is a state organisation or another organisation performing public functions that is acting in Estonia or EU;
- the Client is an EU institution;
- the Client is a credit institution that is active in Estonia and EU, where the provisions of directive 2015/849 are applicable.
- the Client is a physical person that is a resident of Estonia or of another country that has substantial anti-money laundering legislation following the Financial Action Task Force reports.

Use of the simplified control method does not free the company from the obligation to make sure that the transaction is transparent.

4.7 Should the risk of the transaction be considered high or should there be reasons to consider the risk of commercial relations high, a higher-level control method of client identification should be used, by requesting the client to provide additional information and documents that can rule out the risk. Information is also to be provided to the financial inspection of Estonia to get more instructions. Aside from the high-risk level that was given under the risk analysis following the provisions of part 5 of this Document, additional reasons to consider the transaction to be high risk are the following:

- unusual circumstances for the transactions;
- the client operates with high volumes of cash;
- a legal person client has hidden owners or recipient type shares;
- the structure of the legal person is too complex and confusing;
- new or unknown goods are the subject of the transaction and transaction specifics are unusual;
- the transaction is made for anonymity purposes;
- unknown third parties make payments following the transaction;
- other circumstances mentioned in article 37 of the Estonian money laundering and terrorism finance prevention act.

5. Risk evaluation.

5.1 Any Client and his planned transaction are evaluated regarding the risk factor of money laundering and finance of terrorism.

5.1.1 During the risk evaluation the Client is given the risk status, from lowest to highest, by the means of evaluating further risk factors:

- Client corporate structure and field of activity;
- If the Client is a state official or is connected to one;
- If the Client is represented by a legal person;
- If the beneficiary of a physical person is a third party;
- There are problems identifying the beneficiary;
- The Client is connected to low tax jurisdictions;
- The Client is subject to international sanctions;
- The Client is a typical client;
- There is positive experience of cooperation with the Client;
- Term of cooperation;
- Nature of the planned transaction;
- Amount of the transaction;
- Whether the Clients are stable or constantly shifting;
- Problems during identification procedures;
- Whether the goods or property origins are unclear.

5.2 The nature of the transaction must be evaluated to set the risk status.

5.2.1 The transaction may be awarded with a low, medium or high-risk status depending on the following factors:

- The transaction involves currency exchange or purchase of precious metals;
- The transaction involves a private bank;
- The transaction involves alternative payment methods;
- The transaction involves gambling;
- The transaction involves rarities or exclusive goods;
- The transaction involves innovations;
- The transaction involves commercials;
- The transaction involves company establishment or management.

5.3 Geographical circumstances are to be evaluated (to determine a geographical risk).

5.3.1 The transaction may be awarded with a low, medium or high-risk status depending on the following geographical actors:

- The transaction involves low tax jurisdictions. This entails a company registered at the low tax jurisdiction or services provided at the low tax jurisdiction;
- The transaction involves a state that does not cooperate in the field of money laundering prevention and finance of terrorism;
- The transaction involves a state with a high crime rate or trafficking of drugs;
- The transaction involves a state with a high level of corruption;
- The transaction involves a state that is subject to international sanctions;
- Other factors that may increase the geographical risk.

5.4 Along with the risks connected to the Client, risks regarding his partners or associated persons are also evaluated.

5.5 The risk evaluation is performed by giving each risk group a status on a three-point scale:

- Risk is considered low if no category has a risk factor and the transaction is clear;

- Risk is considered medium if there are risk factors, but the transaction itself is clear, though there are suspicions that all of the risk factors together may indicate money laundering or finance of terrorism;
- Risk is considered high if there are multiple risk factors and the transaction itself is not clear.

Overall result is achieved by adding the factor of each category, whereas risks regarding client and partner is multiplied by two and then the whole sum is divided by a factor of 4.

- If the sum is 2 or lower, the risk is low;
- If the sum is 2 to 2,75, the risk is medium;
- If the sum is higher than 2,75, the risk is high.
- If the risk in any category is high, the overall risk is considered high no matter the overall sum.

6. Commercial relationship with the Client

6.1 Any commercial relationship with the Client is initiated only after the Client agreed to act in accordance with the present AML policy.

6.2 Before the start of commercial relationship the following must be set:

- Nature of the planned agreement;
- Terms of the planned agreement;
- Volume of the planned agreement.

Received information is kept in a written form.

6.3 Should there be a representative between a physical or legal person, the company is to ensure that there is actual contact between the client and the representative.

7. Actions in case of suspicions regarding money laundering and obligation to provide information

7.1 Should there be any suspicion before the initiation of commercial relationship or during the use of control methods, that the transactions may be connected to money laundering or finance of terrorism, further cooperation is impossible.

7.2 Any suspicions are registered and analysed by the contact person. The Anti Money Laundering Bureau of Estonia and the Financial inspection of Estonia must be notified immediately of the results of the analysis.

7.3 All information regarding any transactions that is 32000 EUR or higher must be provided to the Anti Money Laundering Bureau of Estonia and the Financial Inspection of Estonia.

7.4 Should the denial to perform the transaction result in damages to the Client or the arrest of a person suspected in money laundering or terrorism, the transaction may be delayed or performed on the condition that the Financial Inspection is informed without delay.

7.5 All the information provided to the Financial Inspection is kept in an archive in accordance with provision 13 of the present document, including the data analysis results.

7.6 Persons suspected of money laundering or the finance of terrorism should not be provided any information regarding the suspicions or notified of them by any other means.

8. Correspondence exchange

8.1 Should it be deemed by the management to be necessary to implement the control method, a correspondence exchange with third parties may be initiated, including banks and other financial institutions, should that allow to gather more accurate information.

8.2 The correspondence exchange must be drawn up in the form of a two-way agreement, including the control methods used.

8.3 There can be no correspondence exchange with shadow banks, unlicensed organisations or with organisations situated in jurisdictions whose legislation is not up to the international standards in the field of Anti money laundering legislation and prevention of the finance of terrorism.

9. Information recording program

9.1 Information recording program sets the obligation for the company employee who performed the transaction to draw up an internal document containing all the specifics of the transaction that must include:

9.1.1 The category of the transactions and the reasons why the transaction may be considered a high-risk transaction;

9.1.2 The details of the transactions, including the volume of the transaction and currency;

9.1.3 The details on the persons involved in the transactions;

9.1.4 The information on the Company employee involved and his signature;

9.1.5 The date of the act;

9.1.6 A written letter from the company management board member or from another authorized person regarding a transaction performed under this act.

9.1.7 Information regarding any additional methods of control used in regard to the transactions;

9.1.8 There is no pre-arranged act form. Acts are made by hand by each employee and are presented to the member of the management board for review.

10. Transaction denial program

10.1 If the Client, despite his obligation, did not present the required documentation in accordance with the control methods, the applicable legislation, and this policy, the Client will be denied in the performance of the transaction.

10.2 Should the Client fail to present information regarding the source of the funds upon the request, the transactions shall also be denied.

10.3 Information regarding the transaction denial must be kept in accordance with provision 13 of this policy, including:

- The information on the circumstances of the transaction denial and account blocking.
- The circumstances for the denial of the start of commercial cooperation;
- Any circumstances regarding the end of commercial cooperation in accordance with provisions 7.1 and 7.2 of the present policy.
- The data that provided the reason that the state authorities were notified in accordance with section 32 of the Money Laundering and terrorism finance prevention act.

10.4 The decision regarding the denial to perform the transaction may be reversed if the Client provides the required information and documents or if such shall be set by the decision of the following organs:

- A control organ of the Republic of Estonia;
- A competent Court of Estonia.

11. Company employees training program

11.1 The program regarding the training of employees in the field of Anti Money Laundering Legislation and Prevention of the finance of terrorism is made in accordance to the applicable legislation and includes proper instructions for the employee regarding the control methods and information analysis. Any employee must be properly instructed by the authorised workers during the period of a month from the start of employment.

12. Internal control review program

12.1 The internal control review program ensures that the employees and members of the company abide by the provisions of the applicable legislation in the field of income legalisation obtained by illegal means and the finance of terrorism. The program ensures that the employees abide by internal company rules and regulations in the field of internal control.

12.2 Internal controls set the following rules:

12.2.1 Regularly, at least once every six months, internal checks must be carried out regarding the proper implementation of internal regulations and applicable legislation.

12.2.2 Disciplina OÜ member of the board must be provided with regular written reports regarding all the violations of internal regulations in the field of money laundering prevention and prevention of the finance of terrorism.

12.2.3 All violations revealed during checks must be properly handled by the means chosen by the management board member.

13. Document maintenance program

13.1 All documents connected to the client identification procedure as well as all the information regarding the start of commercial cooperation must be maintained in the company archive for no less than 5 years.

13.2 All documents that became the reason for notifying the state authorities must be maintained for no less than 5 years.

13.3 All information on the inquiries made in order to abide by the provisions of the applicable legislation must be kept for no less than 5 years from the start of commercial cooperation. If the identity was confirmed by the means of a digital document, then the picture of the person and their signature is kept for no less than 5 years from the date of the end of commercial cooperation.

13.4 The documents must be maintained in a form that allows their written reproduction, so that they would be readily available for financial control or for other state authorities in accordance with the applicable legislation, should they be required for use in civil, criminal, or arbitrary proceedings.

Internal control rules set the confidentiality standards for the information that was received during identification process and other means prescribed by the applicable legislation.