CRPT TRT OÜ

PROCEDURE AND INTERNAL CONTROL RULES FOR THE VIRTUAL CURRENCY EXCHANGE SERVICE PROVIDER

Money Laundering and Terrorist Financing Prevention Act

GENERAL PROVISIONS and DEFINITIONS

These procedure rules (hereinafter **"Guideline"**) regulate the activities of CRPT TRT OÜ (hereinafter "CRPT") for implementing the Money Laundering and Terrorist Financing Prevention Act.

In the Guideline, terms have the following meaning:

Money Laundering- current definition of money laundering in accordance with §4 of Money Laundering and Terrorist Financing Prevention Act.

Terrorist Financing- current definition of terrorist financing in accordance with §5 of Money Laundering and Terrorist Financing Prevention Act.

Beneficial owner- current definition of beneficial owner in accordance with §9 of Money Laundering and Terrorist Financing Prevention Act.

CRPT- the virtual currency exchange service provider who is required to be a person within the meaning of Money Laundering and Terrorist Financing Prevention Act.

Business Relationship- current definition of the business relationship in accordance with §3 of Money Laundering and Terrorist Financing Prevention Act.

Client- current definition of the Client in accordance with §3 of Money Laundering and Terrorist Financing Prevention Act.

Staff member- CRPT employee, CRPT manager, board members, council members.

Contact Person - a person appointed by the Management Board as a Contact Person for the Financial Intelligence Unit.

The Contact Person may be a member of the CRPT Management Board or another staff member.

1. COMPULSORY IMPLEMENTATION OF MONEY LAUNDERING AND TERRORIST FINANCING PREVENTION ACT

As a provider of a virtual currency exchange service, the CRPT commits itself to comply with procedural rules pursuant to §2 (1) of the Money Laundering and Terrorist Financing Prevention Act.

The Management Board of the CRPT will ensure that each Member of the Staff complies with the requirements set in this Guideline, in the Money Laundering and Terrorist Financing Prevention Act and in the legislation issued on the basis thereof. CRPT Personnel must be familiar with and comply with the legislation and relevant Guidelines of the authorities as well as be familiar with changes to legislation and Guidelines.

The Staff Member shall be personally responsible for the fulfillment of the requirements of the Money Laundering and Terrorist Financing Prevention Act and this manual. Non-compliance can lead to termination of employment and malfeasance or criminal punishment.

DUE DILIGENCE MEASURES

1) The CRPT will apply due diligence measures in accordance with the Money Laundering and Terrorist Financing Prevention Act to the appropriate and necessary extent, based on the nature of the CRPT business and the degree of risk of the party involved in the transaction.
2) The CRPT will pay special attention to the activities of the Client and the circumstances that indicate money laundering or terrorist financing, or that are likely to be involved in money laundering or terrorist financing.
3) Prior to establishing a business relationship with the Client, making a transaction, and doing business, the CRPT will apply the following due diligence measures:
    - Client identification, verification of submitted information, data retention and updating.
    - Identifying and verifying the identity of the representative of the Client, and his right of representation. The scope of the mandate given to the representative must be specified, including whether it is a longer-term business relationship or only a

one-off transaction and whether the right of representation allows a business relationship with the CRPT.

- Identifying the beneficial owner.
- Obtaining information on the business relationship and the purpose and nature of the transaction.
- Daily diligence and vigilance in dealing with the Client, including monitoring of transactions conducted in the business relationship, regular checking of the data used to identify the person, updating relevant documents, data and information, and identifying the source and source of funds used in the transaction, if necessary.
- Informing the Contact Person of situations where money laundering or terrorist financing features may occur in the content of the transaction or in the Client's activities and, if possible, non-execution of such transactions.

In the implementation of due diligence measures, if this is not done by means of information technology, the circumstances to be identified are determined based on the original documents provided by the client. If the original document cannot be obtained, a notarized or officially certified document, i.e documents certified by a lawyer. A copy of the document may not be relied on if there is doubt whether the copy is in conformity with the original.

CLIENT IDENTIFICATION

1) Identification must be done for all persons and their representatives who enter into a business relationship with the CRPT.
   Personal knowledge of the Client or his representative or his or her publicity does not preclude compliance with the identification obligation established in the Guideline.
2) When establishing a business relationship with the Client, a representative of the legal or or the nature person, must be identified using information technology tools. For identification and verification purposes, a bank link, ID card, mobile ID, Smart ID, etc. are used, the agreed communication equipment to which only the Client or the Client's representative has access (e.g @eesti.ee or other exclusive e-mail), or / and unique user IDs and authentication tools set by the CRPT. If these documents or e-identification tools are not available, the Client must provide the CRPT with a copy of the identification document. Before making any

transaction, the staff member must first ascertain the identity of the person / representative and the existence of the right of representation.

3) In addition to point 3.2. the following personal data must be provided by the Client (via e-mail or in the form of the exchange platform, unless otherwise specified below):
    1. Natural Person (resident)
        - First and last name;
        - Personal identification code;
        - Name, number, date of issue of the identity document, name of the issuer;
        - Residential address;
        - Occupation or profession;
        - Contact phone number, email address.
    2. Legal Person (resident)
        - The name and registry code of the legal person;
        - Postal address;
        - Field of activity;
        - Contact phone number, email address;
        - The given name, surname, personal identification code or date of birth of the representative (if not shown on the registry card);
        - The basis of the right of representation, in the case of an authorized person the authorization certified by the representative of the legal person and the existence of the right of representation shall be checked from the registration department of Tartu County Court.
    3. Natural Person (non-resident)
        - First and last name;
        - Personal identification code and date and place of birth;
        - Name, number, date of issue of the travel document, name of the issuer;
        - Residential address and postal address;
        - Location address while creating a contact;
        - Occupation or profession;

- Information on whether a person performs or has performed essential functions of public authority or is a close associate or family member of a public authority (ie a person with a national background in the meaning of the Money Laundering and Terrorist Financing Prevention Act);
- A contact telephone number and e-mail address;
- A notarized copy of the page with the travel document image and if needed- a visa or temporary residence permit. A copy must be sent by post.

4. Legal Person (non-resident)
    - The name and registry code of the legal person;
    - The country of location, the name of the country in which the register is located, and the web address; corresponding registers, up-to-date printouts, documentary evidence from CIS and offshore countries also including tax office evidence
    - Actual beneficial owner information;
    - Postal address;
    - Business address;
    - Field of activity;
    - Details of the bank account (s);
    - Contact phone number and email address;
    - The given name, surname, personal identification code or date of birth of the representative (if not shown on the registry card);
    - The basis of the right of representation, in the case of an authorized person, a document certifying the right of representation or authenticated in accordance with the procedure, which has been legalized or certified with an apostille, unless otherwise specified in the international agreement. The notarized copies of the documents must be sent by post.

4) If the value of the transaction executed by the Client exceeds EUR 15,000, the Client must provide the CRPT with a copy or extract from the public utility bill of his / her place of residence, which cannot be older than three months and bearing the name and address of the Client.

5) To verify the information collected, the staff member must use the available records and information on the Internet. In the case of a higher-risk business relationship, information from the advisers or additional documents may be required. If necessary, the staff member will ask for more detailed information about the purpose of the company. If still in the doubt, the Client will be interviewed based on the data collected via the contact phone.

6) The data collected shall be checked and, if necessary, updated at least once every two years.

7) A copy of the document proving the identity of the person who has received the identification on paper shall indicate the name, date of identification and signature of the CRPT staff member who was doing identification. Identification data must be recorded in the CRPT computer system.

4. THE DETERMINATION OF THE NATURAL CLIENT'S RISK PROFILE; THE DETERMINATION OF RISK CATEGORY

A member of staff is required to identify the profile of the Client who is a natural person and determine a risk category. The determination of the risk category of the Client who is a natural person is based on the Client's residency and if he is an actual beneficial owner. In determining the risk category of non-resident natural persons, it is also considered whether the Client is a person with a national background/his /her family member/close associate. If the Client is a person with a national background /his /her family member/close associate, then he / she automatically falls into category III.

4.1 Category I – Low-Risk Category:

A resident or non-resident natural person who is the beneficial owner;

4.2 Category II - Average Risk Category:

A non-resident natural person who is himself the beneficial owner and is not a person with a national background/his/her family member/close associate;

A resident natural person who is not the actual beneficial owner.

4.3 Category III – High-Risk Category:

A resident and a non-resident natural person/member of his/her family member/close associate;

A non-resident natural person who is not the actual beneficial owner.

4.4 The risk category is determined by the member of staff at the start and during the business relationship by adding the relevant category to the Client's data.

4.5 If the Client is in risk category III, enhanced due diligence measures must be implemented (clause 10).

4.6 4.6 If a business relationship with a high-risk (Category III) Client is established, the member of staff will immediately inform the Contact Person via email or telephone assigned by the Board

5. THE DETERMINATION OF THE PROFILE AND RISK CATEGORY OF A LEGAL CLIENT

DETERMINATION

A member of CRPT is required to identify the business profile of a legal Client when establishing a business relationship and to define the risk profile of a legal Client.

The risk category is determined on the basis of the country of the legal person, the field of activity and the transparency of the structure of the management bodies and the owners.

1. **Category I – Low-Risk Category:**

A legal person registered in the Republic of Estonia whose area of activity is defined (excluding fishing industry, construction and repair, wholesale and storage of fuel, retail trade of fuel, wholesale trade of timber, currency and / or payment intermediary, gambling, casino);

A legal person registered in a Member State of the European Union or in Norway, Iceland, Switzerland, whose shares are publicly quoted and the company does not operate in the fishing industry, construction and repair, wholesale and storage of fuel, retail trade of fuel, wholesale trade in timber, currency and/or payment intermediary, gambling, casino;

Government agencies, insurance institutions and pension funds, residential credit institutions, residential local government, residential central bank, residential state social insurance fund, non-residential central government, non-residential insurance institutions and pension funds, non-residential local government, non-residential state social insurance fund, private company daughter resident, financial institution daughter / non-residential, residential insurance institution and pension fund automatically belong to a low risk category.

2. Category II - Average Risk Category:

A legal person registered in a Member State of the European Union or in Norway, Iceland, Switzerland, whose shares are not publicly quoted and the company does not operate in the fishing industry, construction and repair, wholesale and storage of fuel, retail trade of fuel, wholesale trade in timber, currency and / or payment intermediary, gambling, casino;

A legal person registered in the Republic of Estonia whose area of activity is defined (excluding fishing industry, construction and repair, wholesale and storage of fuel, retail trade of fuel, wholesale trade of timber, currency and/or payment intermediary, gambling, casino);

A legal person registered in a Member State of the European Union or in Norway, Iceland, Switzerland, whose shares are publicly quoted and the company does operate in the fishing industry, construction and repair, wholesale and storage of fuel, retail trade of fuel, wholesale trade in timber, currency and / or payment intermediary, gambling, casino; a legal person registered in third countries and in Liechtenstein whose shares are publicly quoted and whose activities are not connected with the fishing industry, construction and repair, wholesale and storage of fuel, retail trade of fuel, wholesale trade in timber, currency and / or payment intermediary, gambling, casino;

3. Category III – High-Risk Category:

A legal person registered in third countries and in Liechtenstein (except for point 5.2.2 (iv));

A legal person registered in a Member State of the European Union or in Norway, Iceland, Switzerland, whose shares are not publicly quoted and the company does operate in the fishing industry, construction and repair, wholesale and storage of fuel, retail trade of fuel, wholesale trade in timber, currency and / or payment intermediary, gambling, casino;

If the Client belongs to risk category III, enhanced due diligence measures must be implemented (p 10).

The risk category is determined by the CRPT staff member at the start and during the business relationship by adding the relevant category to the Client's data.

If a business relationship with a high-risk (Category III) Client is established, the employee will immediately inform the Contact person via email or telephone assigned by the Management Board. In addition, the Contact Person must be informed if the company's business is related to the arms industry, arms sales or brokering.

CLIENT IDENTIFICATION DURING THE BUSINESS RELATIONSHIP

Client identification is required during the business relationship.

The CRPT has the right to suspend the execution of transactions or terminate if, in the event of a suspicion of money laundering occurring during the business relationship, the Client does not submit any documents or data that would disprove such doubt. An assessment of suspicion of money laundering is issued and decided by the CRPT Executive Board or the Contact Person.

IDENTIFICATION AND TRANSACTIONS OF A PERSON WITH A PUBLIC BACKGROUND

1. Persons with a national background are the persons listed in §3 (11) of the Money Laundering and Terrorist Financing Prevention Act who are divided into persons with national backgrounds performing functions assigned by national and international organizations.
2. The Contact Person is responsible for identifying persons with a national background from CRPT Clients and potential clients unless the CRPT Board has appointed another person to do so.

3. Identifying a person with a national background is possible through:
    - Asking the Client

- Using existing public or paid databases and internet search engines; or 3 by requesting or verifying data through the websites of the authorities of the country where the Client is located.
- The establishment of a business relationship with the Client with a national background must be decided by the CRPT Board or the Contact Person. If the business relationship with the Client has been established and the Client turns out to be later or becomes a person with a national background, then it is necessary to inform the Contact Person in writing or in a format that can be reproduced in writing.

SMALL AND HIGH-RISK TRANSACTIONS

1. When executing a transaction, a CRPT staff member must assess the risk of money laundering and terrorist financing and select appropriate due diligence measures in accordance with the Guidelines and implement them.

2. The risk of money laundering and terrorist financing is assessed taking into account the Client's risk and transaction risk.

3. A transaction related risk is considered small if the following circumstances occur:
   - The benefit of the transaction cannot be realized by the Client before one year after the transaction;
   - The transaction is not a quick payment;
   - The contract concluded does not provide for the Client buy-back clause;
   - The following risk factors shall be considered as low while identifying and verifying the Client specified in §34 (2) from point 1 to 6 of the Money Laundering and Terrorist Financing Prevention Act:
   - Client identification is possible based on publicly available information;
   - The Client's ownership and control structure is transparent and permanent;
   - The Client's and accounting activities are transparent;

- The Client is accountable and controllable by an executive authority of the contracting state of the EEA or a contracting state of the European Economic Area, by another authority performing public functions or by a body of the European Community.

4. Client risk is considered high if the Client is:
   - Entered on the UN or European Union list of persons subject to international financial sanctions;
   - A person to whom the CRPT has previously been suspected of being involved in money laundering or terrorist financing;

5. A transaction-related risk is considered high if:
   - The transaction will be made by the Client's representative, who is unable to explain the origin of the money;
   - The transaction will be made by the Client, who is the subject for CRPT prior suspicion that the person may be related to money laundering or terrorist financing;
   - The transaction is to be made in cash;
   - Upon making the transaction, a third party or through a third party the cash deposit is requested;
   - Transactions or operations that comply with the characteristics specified in Appendix 2 and 3 of this Guideline;
   - For high-risk transactions, due diligence measures need to be implemented;
   - In the event of an unusual transaction or circumstance, a member of staff is required to analyze and compare the circumstances of the transaction with the characteristics of the transactions suspected of money laundering and terrorist financing. A member of staff has a duty to verify the legal origin of the property prior to the transaction, at least if the transaction is unusual in the light of the current business relationship with suspicion of money laundering or terrorist financing.
   - Due diligence measures must also be implemented when a low-risk transaction or Client is in doubt as to money laundering or terrorist financing.

IMPLEMENTATION OF SIMPLIFIED DUE DILIGENCE MEASURES

1. Simplified due diligence measures may be applied under the following conditions:
   - To the persons specified in the §34 (2) from point 1 to 6 of the Money Laundering and Terrorist Financing Prevention Act; or
   - if the Client has a written permanent contract; or
   - if the member of staff has no doubts about the correctness of the data submitted by the Client or the legal capacity of the Client; and
   - if the member of staff does not have any suspicion of money laundering or terrorist financing in connection with the transaction; and
   - if the transaction or Client risk can be considered low; and
   - if the Client has a previous business relationship that was created prior to the introduction of this Guideline or the Client has been identified after the introduction of this Guideline in accordance with the Guideline

2. The implementation of simplified due diligence measures:
   - Persons shall be identified in accordance with clause 3 of this Guideline;

3. However, if a member of staff has doubts about the correctness of the information provided by the Client in applying the simplified due diligence measures, a member of staff will perform additional verification. While additional verification, the CRPT employee calls the Client and specifies the Client's data and may ask other verification questions. If it is not possible to carry out the check or it becomes evident during the inspection that the Client is unable to answer the control questions, the transaction will not be conducted with the Client.

4. It is forbidden to apply simplified due diligence measures in case of suspicion of money laundering or terrorist financing at any stage of communication with the Client. If during the implementation of the simplified due diligence measure, a member of the staff suspects money laundering or terrorist financing, a member of staff shall inform the Contact Person by telephone or e-mail.

THE IMPLEMENTATION OF ENHANCED DUE DILIGENCE MEASURES

1. The CRPT member shall apply enhanced due diligence measures when the nature of the situation involves a high risk of money laundering or terrorist financing. Enhanced due diligence measures must be applied if:
    - The Client participating in the transaction has been identified and the information provided has been verified without being in the same place with him; and
    - The identification or verification of the information provided raises doubts as to the veracity of the data provided or the authenticity of the documents or the identification of the beneficial owner; and
    - The Client participating in a transaction, or a member of his or her family, or a close associate is a person with a national background, in another Contracting State of the European Economic Area or a third country; and
    - Features of higher risk transactions occur;
    - In the event of implementation of enhanced due diligence measures, in addition to the usual due diligence measures, at least one of the following enhanced diligence measures shall apply:
    - Identification and verification of the information provided on the basis of additional documents, data or information from a reliable and independent source or from a credit institution registered in Estonia or a branch or credit institution of a foreign credit institution that is registered or has a place of business in a Contracting State of the European Economic Area or a country with equivalent requirements for Money Laundering and Terrorist Financing Prevention Act, and if the identity of the person in the credit institution is in the same place as the person identified;
    - taking additional measures to verify the authenticity of the documents submitted and the accuracy of the information contained there, including their notarial or official confirmation or verifying the accuracy of the data by the credit institution specified in (i) which issued the document; (iii) making a transaction-related first payment through an account opened in the name of a person participating in the transaction with a credit institution registered or established in a Contracting State of the European Economic

Area or in a country subject to equivalent requirements under the Money Laundering and Terrorist Financing Prevention Act.

2. In the event of an unusual transaction or circumstance, a member of staff is required to analyze and compare the circumstances of the transaction with the characteristics of the transactions suspected of money laundering and terrorist financing. A member of staff has a duty to verify the legal origin of the property before the transaction is executed, at least if the transaction is unusual in the light of the current business relationship with suspicion of money laundering or terrorist financing.

3. In the case of transactions with a higher degree of risk, it is necessary to compare the circumstances of the transaction with the features of the transactions suspected of money laundering or terrorist financing and to inform the Contact Person of the suspicion of money laundering and terrorist financing.

MONITORING BUSINESS RELATIONSHIP

12.1 A Member of staff appointed by the CRPT Management Board shall regularly monitor the business relationship with the Client to ensure that the transactions executed are consistent with its business and risk profile. To this end, a member of staff shall:

Regularly monitor the amount of money used in the transaction and the frequency of transactions and, if necessary, identify the origin of assets used in the business relationship and / or transactions; regularly check the legal status of the Client (legal capacity), financial situation, field of activity, ownership information (actual beneficial owner).

12.2 Additionally, a member of staff shall monitor at least once a year:

Client Risk Assessment;

Risk assessment of the country where the Client is located;

Risk assessment of the combined risk

With the Client's risk (risk factors arising from the Client) must be considered: the legal form of the person, the management structure (including trusts, partnerships or other such contractual legal entities, legal entities having bearer shares);

The ownership structure of the company, in particular, those which have no obvious commercial justification and which may make it easier to conceal the final beneficiary;

The field of activity of the Client (Clients involved in the business involving the handling of large sums of cash such as currency exchange offices, cash handlers, high-value merchants, casinos, betting and other companies involved in gambling activities who regularly receive cash payments);

Whether a person or his / her family member or a close associate (Client or beneficial owner) are with a national background;

1) Whether the person is represented by a legal person;

The person's residence, including whether he is a registered person in an offshore region (tax-free and low-tax territories, for example, based on the relevant data provided on the Tax and Customs Board website https://www.emta.ee/et/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-eesti-tulumaksustamine)

Circumstances arising from the experience of communicating with the Client, partners, owners, agents, etc. (eg suspicious transactions identified during an earlier business relationship, suspicious Client behavior, non-filing of required documents);

2) Duration of activity, nature of the business relationship.

Country risk, the risk factors resulting from differences in the legal environment of different countries, the level of crime, and whether international sanctions have been or are being applied against that country or persons in that country.

More risky countries include:

- Subject to international sanctions or embargoes;
- Who do not have sufficient money laundering laws and regulations in line with international standards;

- For whom the financing or support of terrorism has been identified;
- With a high level of corruption or organized crime or other crime (including drug crime);
- Which are tax-free and low-tax offshore financial centers.

Combined risks:

Attention should be paid to the situation in which a staff member indicated a higher risk in several of the above-mentioned risk groups.

The results of the above analysis will be passed in writing form by a member of staff to the Contact Person.

DATA COLLECTION, CONTROL, RETENTION AND UPDATING

Data Collection

The first identification of the Client shall be conducted in accordance with the procedure set out in clause 3 of the Guideline.

During each time when the Client is identified, the CRPT registers on a computer system/ exchange platform:

- The name of the Client, personal identification code, residence, the field of activity or profession; and
- Information on the verification of the data provided by the Client and other data and documents required by the Guidelines.

Data Control

In case of doubt, the validity of the identity document must be checked on the homepage of the Police and Border Guard Board https://www.politsei.ee/et/teenused/isikut-toendavad-dokumendid/index.dot

Data Retention

1. Information provided by the Client and his / her representative, a copy of the Client's and his/her representative's identity document, other documents required by the Client and the

Money Laundering and Terrorist Financing Prevention Act shall be stored digitally on the CRPT computer system (server) or on paper in the location of the CRPT Management Board or at another location designated by the Management Board for at least 5 years after the termination of the contract with the Client.

2. Transaction-related data to suspicion of money laundering or terrorist financing shall be retained by the Contact person in a way that other CRPT staff members have no access to them without the permission of the Contact Person.

3. Data related to suspicion of money laundering or terrorist financing shall be retained. until the expiry of the deadline which is described in paragraph 14.4.1, except if the investigation of the circumstances of the transaction is not completed by this time, in which case the Client and transaction data will be stored until the confirmation of the termination of the investigation.

Updating of data and documents, internal control measures

Updates must be performed at least once every two years. During the data update, a report by a member of staff appointed by the Management Board shall be prepared, which shall include the risks identified in the business activities, the description of the control measures to mitigate the risks and, in the case of shortcomings, how to address them. The report shall be submitted to the Contact Person and the Management Board.

A member of staff responsible for customer relationship (customer manager) will pay much more attention to controlling high-risk (category III) Client's data and business intelligence because of risk analysis. In addition to each annual analysis, the Client manager must continuously assess the potential risks of money laundering and terrorist financing related to the business of the Clients and is obliged to immediately inform the Contact Person about the changes in the risk profile.

Based on the results of the report, the Contact Person draws up a detailed monitoring plan, based on which the Contact Person monitors riskier transactions and monitors the Client profile.

The updated data shall be instantly entered into the CRPT computer system by the Contact Person, with the data available to all other staff members. The Contact Person organizes

management involvement in the process of updating and analyzing the data and takes the results of the report as the basis for the whole risk assessment process, preparation of action plans and counseling for risk reduction.

RESTRICTIONS ON THE EXECUTION OF TRANSACTIONS

No CRPT or Staff member is allowed:

1 Settle in cash;

2 Make a transaction with the Client who has not been identified in accordance with the Guidelines;

3 Make transactions with anonymous or fictitious persons using other names or aliases.

The CRPT and the Staff member refuse to make a transaction with the Client:

- Based on documents or other information submitted, doubts arise about the correctness of the documents or data and the Client does not adequately explain the circumstances that caused the doubts;
- Whose identity or credentials cannot be identified or verified;
- Whose place of residence or profession or activity or profile of activity cannot be identified;
- Who appear on the list of international sanctions or who have been identified by the Financial Intelligence Unit as the person responsible for conducting money laundering or terrorist financing transactions, if such information is disclosed by the Financial Intelligence Unit;
- Due to other circumstances suspects that a person may be involved in money laundering or terrorist financing.
- The refusal to execute a transaction is recorded in the CRPT computer system.

MONITORING AND ANALYSIS OF TRANSACTIONS

1. CRPT member must monitor and analyze whether a transaction or the Client is not involved in money laundering or terrorist financing when executing transactions. The list of features of money laundering or terrorist financing suspicions and abnormal transactions is given in Appendices 2 and 3 of this Guideline (The Financial Intelligence Unit's Guidance on **"The Characteristics of Transactions Suspected of Money Laundering"** and The Financial Intelligence Unit's Guide to **"The Financial Intelligence Unit's Guidance on Characteristics of Transactions Suspected of Terrorist Financing"**)

2. If the Client's activity refers to money laundering or terrorist financing, the Client should be asked for further information to determine the origin of the money. Additional information may be requested orally and/or in writing form, but the information obtained must be recorded and linked to the CRPT computer system with the name of the Client.

3. The Contact Person will analyze Client's transactions, if necessary, to clarify the possible association of the transaction with money laundering or the possibility of the non-legal origin of money.

4. The Contact Person is responsible for managing the risk assessment of money laundering and terrorist financing, must regularly analyze whether there may be risk factors for money laundering and terrorist financing not covered by the Guidelines.

5. While identifying new risk factors, the Contact Person must prepare:
   - An explanation of how new risk factors need to be taken into account within CRPT business and mitigate risks; and
   - A proposal to supplement the Guide and a draft of the new Guidelines.

Contact Person

1. The Contact Person is accountable to the board. The CRPT Board shall immediately inform the Financial Intelligence Unit of the contact details of the Contact Person and of any changes. The Contact Person is a member of the CRPT Management Board unless the CRPT

has appointed another member of staff as a Contact Person. If the Contact Person is a member of the Management Board who is the sole member of the Management Board, the Contact Person shall be accountable to the shareholders.

2. The Contact Person has the right to require all members of the staff to comply with the obligations laid down in the Guidelines and to immediately terminate any breach.

3. The tasks of the Contact Person are:
    - Organizing and collecting information, analyzing and archiving information indicating abnormal or money laundering or terrorist financing suspicions;
    - Providing information to the Financial Intelligence Unit in case of suspicion of money laundering or terrorist financing; Checking CRPT clients and potential clients names of individuals on the UN and EU list of financial sanctions from;
    - Checking the compliance with the Money Laundering and Terrorist Financing Prevention Act and other legislation at least once a year and, if necessary, making amendments to the Guideline;
    - Verification of the availability of technical means to comply with the instructions and to provide timely information;
    - Checking the compliance and the requirements of the law on the prevention of money laundering and terrorist financing and analyzing the results of the inspection and informing the Management Board of the implementation of the Guidelines;
    - Making proposals for the assessment and management of money laundering and terrorist financing risks;
    - Identifying the training needs of staff to prevent money laundering and terrorist financing;
    - Informing the Financial Intelligence Unit of the transfer of the client identification obligation to a third party;
    - Ensuring that the precepts issued by the Financial Intelligence Unit and other authorities are complied by the CRPT;
    - Identifying persons with national backgrounds from clients;
    - Fulfillment of other obligations related to the requirements of the Money Laundering and Terrorist Financing Prevention Act.

4. The Contact Person has the right to examine the documents or other information which is the basis for the establishment of the business relationship or the prerequisites for the performance of his or her tasks.

INTERNAL CONTROL MEASURES

1. The CRPT shall monitor the execution of measures to prevent money laundering and terrorist financing by performing the tasks of the Contact Person in the present Guideline and its Appendix as well as in legislation.

2. In addition, the Contact Person shall conduct at least once a year an internal audit to verify: The compliance of due diligence measures with this Guideline; the compliance of registrations with the requirements of this Guideline; other requirements for combating money laundering and terrorist financing; compliance of the Business Conduct Tracking Operations conducted under this Guideline, compliance with the Guideline and Guidelines of Competent Authorities; Need of training for staff

3. The Contact Person shall prepare a written report on the conduct of internal control. The report includes:
    - Purpose of control;
    - Time of the check
    - Name and title of the person who conducted the control
    - Description of the inspection carried out
    - Analysis of test results or general conclusions and analysis of performed controls
    - In the case of deficiencies, a description of the deficiencies and the risks involved.
    - Time needed to correct deficiencies, recommended actions to correct deficiencies
    - When performing a control, the Contact Person will include in the control report an analysis of the results and a list of measures taken to address the deficiencies, indicating the actual time taken to address the deficiencies.

4. In conducting ongoing and annual additional checks, the Contact Person is entitled to:
    - To monitor the work of employees and to obtain the necessary technical means;
    - To demand an immediate end to the violation of money laundering and terrorist financing requirements;
    - Make suggestions to remedy the deficiencies found during the inspection, i.e. to amend and supplement the procedural rules.

MANAGE COMPLIANCE OBLIGATIONS

1. The staff member shall inform the Contact Person of any of the following situations:
    - Any transaction where a cash commitment of more than EUR 32,000 or an equivalent amount in another currency is settled in cash, regardless of whether the transaction is made in a single payment or in several interlinked payments;
    - Money laundering or terrorist financing. A list of features of money laundering or terrorist financing suspicions and abnormal transactions is provided in Appendices 2 and 3 of this Guideline (The Financial Intelligence Unit's Guidance on "The Characteristics of Transactions Suspected of Money Laundering" and The Financial Intelligence Unit's Guide "The Financial Intelligence Unit's Guidance on Characteristics of Transactions Suspected of Terrorist Financing".)
    - Cases that indicate a violation of the Code by the CRPT;
    - If the Client does not submit the identity document, information about his / her place of residence and field of activity and, in the case of representation, the document on which the right of representation is confirmed.

2. No person (including a colleague) other than the Contact Person or the CRPT Board may be informed of the discovery of a transaction suspected of money laundering or terrorist financing. Informing the Client of a notice sent to the Financial Intelligence Unit about money laundering or suspicion of terrorist financing is prohibited.

3. Upon becoming aware of a transaction suspected of money laundering or terrorist financing, the Contact Person shall analyze the content of the information received in relation to the Client's current transactions and other known information and, if necessary, consult with the member of the CRPT Board as to whether it may be a transaction indicating money laundering or terrorist financing.

4. Data on a transaction suspected of money laundering or terrorist financing shall be retained by the Contact person in such a way that no other CRPT staff member has access to them without the written permission of the Contact Person.

5. When identifying a transaction, the features of which refer to money laundering or terrorist financing:
   - The Contact Person shall promptly inform the Financial Intelligence Unit of a suspicious transaction verbally, in writing or in a format that can be reproduced in writing. If the notice is delivered orally, the Contact person shall repeat it in writing at the latest within the next working day;
   - The Contact Person authorizes the CRPT employee to complete the pending transaction after: written permission from the Financial Intelligence Unit to execute the transaction; or consultation of a member of the management board of the CRPT if the postponement of the transaction could cause significant damage, in which case a written notice shall be sent to the Financial Intelligence Unit immediately after the transaction.

6. The Contact Person shall inform the Financial Intelligence Unit of any notice to the CRPT Board within three working days of the date of dispatch of the notification.

7. Upon request of the Financial Intelligence Unit, the Contact Person shall provide the Financial Intelligence Unit with additional information on the circumstances of the transaction suspected of money laundering or terrorist financing and on the client, if such information exists in the CRPT.

8. Additional requirements to comply with the reporting obligation in case of suspicion of money laundering and terrorist financing may arise from the instructions of the Financial Intelligence Unit, which the Contact Person must inspect independently at least once a year.

9. CRPT retains all notices of suspicious and unusual transactions received from employees for at least 5 years from the date of the notification, as well as the information and other related documents collected for the analysis of these notifications, and notifications to the Financial Intelligence Unit, together with the time of transmission of the notice and the data of the employee who posted.

10. Pursuant to §52 (2) of the Money Laundering and Terrorist Financing Act, the obligation to notify the debtor in good faith in cases of suspicion of money laundering and terrorist financing is not deemed to be fulfilled, and the provision of relevant information to the Financial Intelligence Unit for violation of a confidentiality requirement imposed by law or contract, and for those who have fulfilled the obligation to notify, shall not be subject to legal or contractual liability for the publication of such data.

TRAINING AND NOTIFICATION OF WORKERS

1. The Contact Person will periodically train and inform CRPT staff members to raise staff awareness of:
   - The typical cases of suspicious and unusual transactions and the preventive measures applied;
   - Compliance with legal requirements;
   - Sanctions for non-compliance with legal requirements;

2. For a new employee, the Contact Person or an authorized CRPT employee will introduce the Guideline and inform the employee about the application of due diligence measures, money laundering suspicion and requirements to inform the Contact Person;

3. The employee may require the Contact person to receive (additional) training on money laundering and terrorist financing or to clarify how to prevent money laundering and terrorist financing in the CRPT business.

4. The Contact Person regularly assesses the training needs of staff for money laundering and terrorist financing and reports to the Bureau on this.

MONITORING

1. The Contact Person monitors compliance with the Rules. The activities of the Contact Person are supervised by the Management Board unless otherwise provided in this Guideline.

2. The Contact Person must monitor the assessment and management of risks, the collection and storage of data and the fulfillment of reporting obligations. The Management Board exercises supervision over the obligation to inform the Management Board.

3. The Contact Person has the right to access the CRPT computer system, documents and other information for the performance of his tasks.

4. The Contact Person has the right to verify that CRPT staff members comply with money laundering and anti-terrorist financing requirements and demand an immediate end of the violations.

5. The CRPT Board and Contact Person shall cooperate with the Financial Intelligence Unit by providing the abovementioned authority with information on the implementation of the Guidelines and other related circumstances upon their request.

Appendix 1 The Financial Intelligence Unit's Guidance on "The Characteristics of Transactions Suspected of Money Laundering"

Appendix 2 The Financial Intelligence Unit's Guide "The Financial Intelligence Unit's Guidance on Characteristics of Transactions Suspected of Terrorist Financing"

Appendix 3 Familiarization with the Guideline

I have read the CRPT OÜ Money Laundering and Terrorist Financing Prevention Guideline and undertake to comply with it.

Maksym Supruniuk	01.10.2018	
First name and Surname	Date	Signature