Blackfort Tech Estonia OÜ

Rules of Procedure
for prevention of money laundering and terrorist financing

CONTENTS

Approved by a resolution of the management board on 29.06.2020

1. General provisions

1.1. These Rules of Procedure lay down internal security measures for conducting due diligence and detecting suspicious and unusual transactions in the services provided by Blackfort Tech Estonia OÜ ("**Company**") that are within the scope of the license for the provision of virtual currency services.

1.2. The license for the provision of virtual currency services includes custodial exchange between virtual currency and fiat currency and vice versa and between virtual currencies, as well as the provision of safekeeping or generation of private keys of the customers within the context of the provision of a virtual currency wallet service.

1.3. All relevant employees should know and follow the requirements set out in the Money Laundering and Terrorist Financing Prevention Act (**MLTFPA**), the guidelines on the characteristics of suspicious transactions possibly involving money laundering and terrorist financing, other guidelines on compliance with the MLTFPA pertaining to the activities of the Company as well as these Rules of Procedure.

1.4. All relevant employees should keep themselves up to date with any amendments to the legislation and with other legal acts published on the website of the Financial Intelligence Unit (**FIU**) at https://www2.politsei.ee/en/organisatsioon/rahapesu-andmeburoo/.

1.5. A copy of these Rules of Procedure shall be available to all relevant employees.

2. Definitions

2.1. **What is money laundering?**

2.1.1. Conversion or transfer of property derived from criminal activity, or, property obtained instead of such 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 actions.

2.1.2. The acquisition, possession or use of property derived from criminal activity, or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein.

2.1.3. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity.

2.2. **What is terrorist financing?**

The allocation or raising of funds to plan or perform acts which are deemed to be acts of terrorism or to finance operations of terrorist organisations, or in the knowledge that the funds allocated or raised will be used for the aforementioned purposes.

2.3. **What is a risk country?**

Countries or regions of interest where the risk of money laundering or terrorism are high. A risk country is a country or jurisdiction that:

2.3.1. According to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective anti-money laundering and combating the financing of terrorism (**AML/CFT**) systems.

2.3.2. According to credible sources has significant levels of corruption or other criminal activity.

2.3.3. Is subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations.

2.3.4. Provides funding or support for terrorist activities, or that has designated terrorist organisations operating within their country, as identified by the European Union or the United Nations.

2.4. What is a high-risk country?

A country specified in a delegated act adopted on the basis of Article 9(2) of Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The current list is available here: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.254.01.0001.01.ENG

2.5. Who is a politically exposed person (PEP)?

A natural person who performs or performed prominent public functions as well as their family members and close associates. Persons who, by the date of entry into a transaction, have not performed any prominent public functions for at least one year, as well as their family members or close associates shall not be considered politically exposed persons.

2.5.1. For the purposes of these Rules of Procedure, the following persons shall be persons performing prominent public functions:

a) State, head of government, minister and deputy or assistant minister;
b) a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors, or of the board of a central bank;
c) an ambassador, a chargé d'affaires or a high-ranking officer in armed forces;
d) a member of an administrative, management or supervisory body of a State-owned enterprise;
e) a director, deputy director or member of the board, or equivalent function, of an international organisation, except middle-ranking or more junior officials.

2.5.2. The following persons are considered family members of a person performing prominent public functions:

a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or a local politically exposed person;
b) a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or local politically exposed person;
c) a parent of a politically exposed person or local politically exposed person.

2.5.3. The following persons are considered close associates of a person performing prominent public functions:

a) 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 politically exposed person or a local politically exposed person;
b) 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 politically exposed person or local politically exposed person.

2.5.4. The following persons shall be local politically exposed person:

a) a person who is or who has been entrusted with prominent public functions in Estonia, another contracting state of the European Economic Area, or in an institution of the European Union.

2.5.5. How the relevant employee should check if the customer is a PEP:

The relevant employee should make a research using the potential customer's full name. In case, there are several similar results, the relevant employee must use another identifier (date of birth etc.) to be sure that the result found matches with the potential customer.

To check the relevant employee should use generally known internet research engines and databases the Company has access to. For example, the relevant employee is able to check the PEP status of the potential customer using the NameScan database available at: https://namescan.io/FreePEPCheck.aspx

2.6. What is the MLTFPA?
The legal act that regulates the activities of credit and financial institutions, other undertakings and institutions specified in the Money Laundering and Terrorist Financing Prevention Act and the Financial Intelligence Unit which involve the prevention of money laundering and terrorist financing. In Estonian: *Rahapesu ja terrorismi rahastamise tõkestamise seadus* (RT I, 17.11.2017, 2)

2.7. What is the International Sanctions Act?
This legal act regulates the national imposition of international sanctions, the implementation and the supervision thereof where the imposition of international sanctions has been decided by the European Union, the United Nations, another international organisation or the Government of Estonia.

2.8. Who is a customer?
A person or a legal entity who uses, or has used, one or several services offered by our Company.

2.9. Who is a relevant employee?
A person who is conducting KYC/AML measures about the customer in our Company.

2.10. What is a business relationship?
For the purposes of these Rules of Procedure, a business relationship is a continued contractual relationship with a customer.

2.11. What is a transaction monitoring?
Every single investigation conducted by an employee about a customer.

2.12. What is an occasional transaction?
It is a transaction that occurs outside the scope of the business relationship and that consists of amounts equivalent to EUR 15 000 or more, whether that transaction is carried out in a single operation or in several operations which appear to be linked; or is a transaction that consists on a transfer of funds that exceeds EUR 1,000 carried out by electronic means on behalf of a payer through a payment service provider, with a view to making funds available to a payee through a payment service provider, irrespective of whether the payer and the payee are the same person and irrespective of whether the payment service provider of the payer and that of the payee are one and the same.

2.13. What is a transaction monitoring?
Every single investigation conducted by an employee about a customer.

2.14. Who is an ultimate beneficial owner of a legal entity (UBO)?
Ultimate beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal entity or arrangement. Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control. This definition should also apply to beneficial owner or a beneficiary under a life or other investment-linked insurance policy. Without derogating from the above, UBO is a private individual owning or controlling more than 25% of a legal entity.

2.15. What is the Financial Intelligence Unit?
A separate structural unit of the Estonian Police and Border Guard Board that exercises supervision and uses enforcement powers of the state on the grounds and pursuant to the procedure prescribed by law. Postal address: Rahapesu andmebüroo (FIU), Tööstuse 52, 10416 Tallinn; e-mail: rahapesu@politsei.ee Web-based reporting form: https://www.politsei.ee/et/saada-teade

3. Standard procedure for customer identification and verification (on-boarding customers)

3.1. The relevant employee must identify all customers who wants to use our Company's services on the basis of an identity document and shall record the identification and transaction data regardless of whether the customer is a regular customer or not.

3.2. A person must be identified:

a) prior to establishing a business relationship;

b) upon suspicious customer behaviour;
c) upon verification of information or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered beforehand while updating relevant data;
d) again upon making or mediating occasional transactions outside a business relationship where a payment of over 15 000 euros or an equal amount in another currency is made, regardless of whether the financial obligation is performed in the transaction in a lump sum or in several related payments over a period of up to one year, unless otherwise provided by law.

3.3. If the customer is a private individual, he or she must provide:

a) their full name;
b) their personal identification code or, if none, the date and place of birth and the place of residence;
c) a copy of an identity document according to 3.4;
d) if the customer is in fact representing another private individual being the real customer (under a power of attorney, or in the case of inheritance, or any other way) information on the identification and verification of the right of representation and scope thereof and, where the right of representation does not arise from law, the name of the document serving as the basis for the right of representation, the date of issue, and the name of the issuer.

3.4. The following valid documents serve as basis for identification:

a) an identity card;
b) a passport;
c) a diplomatic passport;
d) an ID card of the citizen of the European Union;
e) a driving licence if the document shows the name, photo or face image, signature or signature image and date of birth or personal identification code of its holder.

3.5. In identifying a person, the relevant employee is obliged to check the validity of the identity document, make sure the person matches the information on the document and check the age of the person. If in doubt about the identity of the person, the relevant employee is obliged to request additional information about the person. Upon sending a document that does not match the person or is invalid, the relevant employee must refuse the customer registration and notify the Compliance Officer.

3.6. The relevant employee verifies the correctness of the customer data, using information originating from a credible and independent source for that purpose. Where the identified person has a valid document specified in section 3.4 or an equivalent document, the person is identified and the person's identity is verified on the basis of the document or using means of electronic identification and trust services for electronic transactions, and the validity of the document appears from the document, or can be identified using means of electronic identification and trust services for electronic transactions, no additional details on the document need to be retained.

3.7. If the customer is an Estonian legal entity (for example a company), it must provide:

a) the name or business name of the legal person;
b) the registry code or registration number and the date of registration;
c) the names of the director, members of the management board or other body replacing the management board, and their authorization in representing the legal person;
d) the details of contact information to the legal person.

3.8. If the customer is a foreign legal entity (for example a company), it must provide in addition to the information in section 3.7Error! Reference source not found., a Commercial Registry (or Company House or similar, depending of the country of origin) extract for the legal entity authenticated by a public notary and/or legalised and/or certified with an Apostille, unless otherwise provided for in an international agreement also showing the rights of representation for that legal entity.

3.9. The relevant employee identifies a legal person based on a registry card of a relevant register or a registration certificate of a relevant register, or another document equal to such card or certificate.

3.10. The relevant employee must identify the beneficial owners (UBOs) and, for the purpose of verifying their identities, taking measures to the extent that allows the relevant employee to make certain that he/she knows who the beneficial owners are, and understands the ownership and control structure of the customer, or of the person participating in the transaction.

3.11. The relevant employee verifies the correctness of the information of a legal entity, using the information originating from a credible and independent source for that purpose. When the relevant employee is able to verify the information through such direct access, the submission of the documents specified in section 3.9 does not need to be demanded from the customer.

3.12. A representative of a legal person of a foreign country must, at the request of the relevant employee, for example when the right of representation does not appear in the submitted document/s, submit a document certifying his or her powers (a power of attorney), which has been authenticated by a public notary and/or legalised and/or certified with an Apostille, unless otherwise provided for in an international agreement.

3.13. The relevant employee may ask additional information about the customer in case of any suspicion about the customer's identity information or the customer's behavior. Such additional information asked should be relevant to the raised risks which, when obtained, may prove that the risks are in fact explainable.

4. Procedure for identification of person and verification of data using information technology means

4.1. The relevant employee must identify a person and verify data with the help of information technology means when a business relationship is established with a person from a contracting state of the European Economic Area or whose place of residence or seat is in such a country and whose total sum of outgoing payments relating to a transaction or a service contract exceeds 15 000 euros per calendar month or, in the case of a customer who is a legal person, 25 000 euros per calendar month; and/or when the due diligence measures are not applied while being physically in the same place as the person or their representative.

4.2. The relevant employee must identify a person and verify data with the help of information technology means where a business relationship is established with an e-resident or a person from a country outside the European Economic Area or whose place of residence or seat is in such country and where the due diligence measures are not applied while being physically in the same place as the person or their representative.

4.3. When identifying and verifying customer's data with the help of information technology means, the relevant employee must comply with the technical requirements and procedure established by the regulation of the Ministry of Finance, which can be found here. The requirements are further included in the following subsections after the table.

4.4. Summary of different AML measures to be applied to a single customer:

Different AML levels that may additionally apply to a single customer	AML measures
1st level – any monetary amount when onboarding a customer.	Clause **3.1** is the same as clause **3.2 a)** but with more detailed explanation. The AML due diligence level (simplified, standard or enhanced) will depend on the risk assessment for that customer. The AML check is done based on the documents and information collected by the Company. Clause **4.2** determines that the verification has to be done "with the help of ICT means" in case of residents of a country outside the EEA.
2nd level – over 15 000 euros per year in cash as occasional transactions	Clause **3.2 d)**: When the customer's transactions are over this limit, the customer must be verified again to ensure that there is still no risk of money laundering or financing of terrorism.

	The AML check is done based on the documents and information collected by the Company. Only non-EEA citizens need to be verified "with the help of ICT means".
3rd level – over 15 000 euros per month (25 000 euros per month if the customer is a legal entity).	Clause **4.1**: requirement applicable to a person from a contracting state of the European Economic Area when the monetary thresholds are passed, the verification has to be done "with the help of ICT means" and not just with the documents collected from the customer.

4.5. When the Company needs to identify and verify person's data with information technology means, the Company must use a document intended for the person's identification and comply with the following preconditions:

a) Use highly reliable technical means which consists of a working camera, microphone, the hardware and software required for digital identification and an internet connection of adequate quality;

b) Use information technology means that allow to compare biometric data. Biometric data includes facial image, fingerprint images, signature or image of signature and iris images;

c) Receive from the customer the confirmation that s/he has read the information about the use of information technology means and agree to the conditions of identification and verification of his/her identity with information technology means;

d) Receive confirmation from the customer that s/he carries out the identification an verification procedures using information technology means personally, that the data submitted is true and complete and that s/he meets the conditions established by the Company for the establishment of the business relationship and the conclusion of occasional transactions;

e) Receive agreement from the customer on the applicability of Estonian law;

f) Request the person (if foreigner) to show in front of the camera the personal data page of the valid travel document issued by the foreign country.

4.6. The identification and verification of a customer using information technology means is unsuccessful if any of the following occur:

a) The person intentionally submitted data that does not correspond to the identification data entered in the identity documents database or does not coincide with the information or data obtained with other procedures;

b) The session expires or is interrupted during the process of identification and verification using information technology means. Session expires when the person has not completed any activity for 15 minutes;

c) The person has not given the confirmations identified in section 4.5;

d) The person refuses to comply with the instructions regarding framing the face and document while using the information technology means: The person's head and shoulders must be visible and framed, the face must be clear of shadows and uncovered, clearly distinguishable from the background and other objects, and recognisable;

e) The person uses the assistance of a third person without the Company's permission;

f) There is suspicion of money laundering or terrorist financing.

4.7. The relevant employee prepares the client profile and the risk profile based on the identification questionnaire, interview, other accessible information and the systematised collection and analysis of data and clarification of facts. Additionally, the relevant employee must give an opinion of the results of the procedure for onboarding using the information technology means and make a proposal on the regime of monitoring business relationships to be applied to the person. The opinion of the relevant

employee of the service provider is the basis on which the decision to establish a business relationship is made.

4.8. The Company shall send an identification questionnaire to the person that wishes to become a costumer. The Company can authorise that the person uses the assistance of another person to eliminate any technical problems when the identification questionnaire is carried out. The relevant employee of the service provider must assess the answers given in the identification questionnaire and record his or her opinion and the circumstances that are the basis thereof in the client profile and risk profile. The questionnaire can be recorded as video, according to the requirements of section 4.11.

In case the person is a natural person, the answers to the questionnaire must indicate the following data:

a) residential address;

b) activity profile;

c) area of activity;

d) purpose and nature of establishment of a business relationship;

e) connection of the person's economic or family interests with Estonia;

f) expected volumes of the services used by the person in appropriate cases;

g) the beneficial owner;

h) whether the person is a politically exposed person;

i) other important information.

In case the person is a legal entity, the answers to the questionnaire must indicate the following data:

a) business name;

b) registry code;

c) location and places of operation, including branches located in foreign countries;

d) the legal form;

e) legal capacity;

f) lawful and contractual representatives;

g) beneficial owner(s) and whether the beneficial owner is a politically exposed person;

h) economic connections with Estonia, contracting states of the European Economic Area and third countries;

i) most important business partners;

j) activity profile;

k) main and secondary areas of activity, purpose and nature of establishment of a business relationship and other important information.

4.9. The relevant employee shall conduct an interview for identification and verification of a person's data during which the relevant employee asks partly structured questions, proceeding from the results of the questionnaire. The relevant employee must carry on the mandatory interview for the establishment of a business relationship in real time. The Company can authorise that the person uses the assistance of another person to eliminate any technical problems when the identification questionnaire is carried out. The relevant employee must assess the person's reaction during the interview, the reliability of the information and data provided by the person with the data obtained through other procedures, and record his/her opinion and the circumstances that are the basis for the person profile and risk profile, which must be reproducible in writing.

4.10. The Company has to allow for digital identification of a person and digital signing.

4.11. The Company must ensure that when video is used (e.g. the real time interview from 4.9), the transmission of clear, recordable and reproducible synchronised sound and image, which is sufficient to

understand the transmitted content unambiguously and reliably, is guaranteed. The video has to be recorded in a way that allows for it to be reproduced with a quality equal to the initial transmission.

4.12. The data collected from the questionnaire, identification of a person, unsuccessful identification of a person, and mandatory real time interview must be recorded with the following requirements:

a) contain a time stamp, which must be tied to the data concerning it in such a manner that any later changes in data, the person who made the changes, and the time, manner and reason thereof can be identified;

b) contain the person's IP address;

c) contain the personal identification code of the person to be identified;

d) contain the birth date and place and country of residence (if there is no personal identification code);

e) be reproducible within five years of the end of the business relationship.

4.13. Inspection of the performance of the identification of person and verification of data using information technology means is done by the Compliance Officer according to section 16 of these Rules of Procedure.

5. Simplified and Enhanced Due Diligence Procedure

5.1. The Company may apply simplified due diligence if a factor characterizing a lower risk has been established and at least the following criteria are met:

a) a long-term contract has been concluded with the customer in writing, electronically or in a form reproducible in writing;

b) payments accrue to the obliged entity in the framework of the business relationship only via an account held in a credit institution or the branch of a foreign credit institution registered in the Estonian commercial register or in a credit institution established or having its place of business in a contracting state of the European Economic Area or in a country that applies requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council;

c) the total value of incoming and outgoing payments in transactions made in the framework of the business relationship does not exceed 15 000 euros a year.

5.2. Before the application of simplified due diligence measures, factors referring to a lower risks are taken into account and the obliged entity determines whether these factors will be implemented on the whole, in part or as separate grounds.

5.3. Upon assessment of factors referring to a lower risk, the following is deemed a situation reducing risks relating to the customer type:

a) the customer is a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the beneficial owner;

b) the customer is a legal person governed by public law established in Estonia;

c) the customer is a governmental authority or another authority performing public functions in Estonia or a contracting state of the European Economic Area;

d) the customer is an institution of the European Union;

e) the customer is a credit institution or financial institution acting on its own behalf or a credit institution or financial institution located in a contracting state of the European Economic Area or a third country, which in its country of location is subject to requirements equal to those established in Directive (EU) 2015/849 of the European Parliament and of the Council and subject to state supervision;

f) a person who is a resident of a country or geographic area having the characteristics specified in section 5.4.

5.4. Upon assessment of factors referring to a lower risk, at least the following situations where the customer is from or the customer's place of residence or seat is in, may be deemed a factor reducing geographic risks:

a) a contracting state of the European Economic Area;

b) a third country that has effective AML/CFT systems;

c) a third country where, according to credible sources, the level of corruption and other criminal activity is low;

d) a third country where, according to credible sources such as mutual evaluations, reports or published follow-up reports, AML/CFT requirements that are in accordance with the updated recommendations of the Financial Action Task Force (FATF), and where the requirements are effectively implemented.

5.5. The relevant employee shall undertake enhanced due diligence (EDD) if there is a higher risk of money laundering or terrorist financing such as:

a) there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
b) the customer is a politically exposed person;
c) the customer is from a high-risk third country or their place of residence or seat or the seat of the payment service provider of the payee is in a high-risk third country;
d) the customer is from a risk country, or from a territory that is considered a low tax rate territory.

5.6. Other factors that are referring to a higher risk pertaining to the customer:

a) When there are unusual factors in the customer onboarding, or when there are unusual transactions patterns without clear economic or lawful purpose;
b) Customer is a legal person or a legal arrangement, which is engaged in holding personal assets;
c) Customer is a cash-intensive business;
d) The customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;
e) The ownership structure of the customer company appears unusual or excessively complex, given the nature of the company's business.

5.7. Other factors that are referring to a higher risk pertaining to the product, service, transaction or delivery channel:

a) Products/services that favours anonymity;
b) Payments received from unknown or unassociated third parties;
c) A business relationship is established without the customer or the customer's representative being physically met in the same place except when a document issued by the Republic of Estonia for digital identification of a person or another electronic identification system with assurance level 'high';
d) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

5.8. The relevant employee must identify what the risks are in every particular case and undertake all appropriate measures to mitigate those risks. Depending on the case, the relevant employee may apply one or several of the following due diligence measures:

a) verification of information additionally submitted upon identification of the person based on additional documents, data or information originating from a credible and independent source;

b) gathering additional information on the purpose and nature of the business relationship, transaction or operation and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;
c) gathering additional information and documents regarding the actual execution of transactions made in the business relationship in order to rule out the ostensibility of the transactions;
d) gathering additional information and documents for the purpose of identifying the source and origin of the funds used in a transaction made in the business relationship in order to rule out the ostensibility of the transactions;
e) making of the first payment related to a transaction via an account that has been opened in the name of the customer participating in the transaction in a credit institution registered or having its place of business in the European Economic Area or in a country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council are in force;

6. Collecting data and record-keeping

6.1. Our Company is obliged to retain all records about our customer and our customers' behaviour in such a way that it can always be presented to inspectors checking the recorded transactions.

6.2. The relevant employee shall put his or her name and, if the document is in a paper format, his or her signature at the end of each entry.

6.3. The Compliance Officer is responsible for keeping all relevant data.

6.4. The relevant data includes:

a) information about the circumstances of refusal of the establishment of a business relationship or the completing an occasional transaction;

b) information if it is impossible to take the due diligence measures using information technology means;

c) originals or copies of the documents that serve as a basis for the establishment of identity and verification of the submitted information;

d) the transaction date or period and a description of the substance of the transaction;

e) the list of payment accounts kept in the name of the Company, along with each payment account's unique feature and the account manager's name.

6.5. The personal data of a customer, a customer's transaction and other relevant information must be stored for no less than 5 years after termination of the business relationship.

6.6. If a customer fails to submit all necessary documents and relevant information, or, if on the basis of the documents provided the relevant employee has a suspicion that money laundering or terrorist financing might be involved, the relevant employee shall not make a transaction with that customer and shall immediately inform the Compliance Officer and record as many customer details as possible that will later help to identify the customer.

7. Risk based approach

7.1. The relevant employee analysing the customer and his/her behaviour should undertake investigative efforts that are proportional to the risk and complexity of the case and collect evidence using observations gathered in the case.

7.2. If the relevant employee identifies any additional risks, they will need to conduct investigative research to understand these risks in the context of the case.

7.3. Additional evidence will be needed to support the review and understanding if additional risks are identified.

7.4. The following questions may help to determine whether a transaction is suspicious or whether there is a risk of money laundering or terrorist financing:

a) Is it inconsistent with the customer's known activities?
b) Is the size of the transaction inconsistent with the normal activities of the customer as determined at the initial identification stage?
c) Are there any other transactions linked to the transaction in question of which our Company is aware of and which could be designed to disguise money and divert it into other forms of other destinations or beneficiaries?
d) Is the transaction rational for the customer?
e) Has the customer's pattern of the transactions changed?
f) Is the customer's proposed method of payment unusual in the context of the services provided by the Company?

8. Interaction with the customer

8.1. The relevant employee may contact the customer to clarify the information given or ask for additional information, which is needed for the customer identification, or to address the risks identified.

8.2. The relevant employee should not request unnecessary or irrelevant information. A request for additional information must be related to the risks of the case, and after receiving the customer's response, the relevant employee may close or report the case to the Compliance Officer. If the risk of money laundering or terrorist financing is very high, the relevant employee shall report the case to the Compliance Officer without asking additional information from the customer.

8.3. The relevant employee shall never express themselves using words that give a reason for the customer to understand that his/her activity is suspicious and may be a subject for further report to the Compliance Officer.

9. Monitoring the business relationship

9.1. A transaction monitoring shall be initiated based on a behaviour trigger of the customer or manually by the relevant employee or by the Compliance Officer. A relevant employee must investigate every initiated case.

9.2. The relevant employee cannot be working on a case if the customer in question is a close person to that relevant employee, or a customer that is in any other way connected with that relevant employee.

9.3. The relevant employee should determine what the risks of the case are. Each risk should be addressed and documented.

9.4. The relevant employee must conduct a pre-research and check whether the customer was checked previously and what were the concerns earlier.

9.5. The relevant employee must conduct customer research to determine the customer's profile and identify the source and origin of the funds used in a transaction.

9.6. The relevant employee must conduct an activity research of the customer and determine whether it is in line with the customer profile or if the behaviour seems suspicious. Activity research includes all observations about the customer's behaviour and any red flags in the activity.

9.7. The relevant employee must conduct research on all the counterparties if it is applicable in the case.

9.8. The case review may vary on the evidence needed to be collected about the customer and his/her activity. The relevant employee should use a risk-based approach to address the risks proportionally.

9.9. The relevant employee must document all the findings about the customer and customer's behaviour which support the decision of the relevant employee about closing or reporting the case to the Compliance Officer.

10. Understanding risk profile of a customer and risks relating to new and existing technologies

10.1. During the monitoring of the business relationship, the relevant employee must collect enough evidence to mitigate the risks alerted. For this reason, the relevant employee should research and use the following information:

a) Source of wealth or the source of fund of the transaction (employment status, role or title in a company, employer, approximate salary, additional source of income, industry type etc.);
b) The customer's age;
c) Location of the customer and the customer's counterparties;
d) The history of the customer's transactions;
e) The type of transactions;
f) Any negative information associated with the customer;
g) Any factors that cause the customer to be considered a high risk;
h) The relationship between the customer and the customer's counterparties;
i) The relationship between the customer and customer's place of residence.
j) Other information which helps to understand the customer, the customer's activity and its counterparties.

10.2. The relevant employee shall always be aware that new, existing and emerging technologies may give the customer a possibility to hide his or her real identity or to make a fraud. Therefore, the relevant employee shall assess the risk of new and emerging technologies and address them within the process of onboarding the client and within the transaction monitoring.

10.3. The relevant employee shall also collect information about the devices the customer uses and their location and add this to the customer KYC file.

10.4. The relevant employee shall also use proxy piercing to identify whether the user is attempting to hide their location and add this to the customer KYC file.

10.5. The relevant employee must cross-check the customer through the internal and external databases of device fingerprints, address, name, e-mail, ID code and all other data that is available in order to detect double registrations or multiple accounts of the customer.

10.6. The relevant employee shall record every virtual currency wallet address that is either used to deposit into or withdraw from the system. They shall all be added into the same virtual currency addresses cluster.

11. Decision-making

11.1. After each transaction monitoring review, the relevant employee will make a final decision about whether to report the case to the Compliance Officer or close the case, based on the evidence collected for the case, and provide a final conclusion that supports the decision made.

11.2. While making a final decision, the relevant employee should:

a) Finish the research about the customer, the customer's behaviour and the customer's counterparties;
b) Understand the evidence collected and look for indications of unusual activities;
c) Consider each piece of evidence on its own and consider all evidence at the same time;
d) If two pieces of evidence contradict each other, look at them together;
e) Identify which pieces of evidence have the greatest impact on your analysis;
f) Identify each piece of evidence that has the least impact on your analysis;
g) Determine which theory is most strongly supported by the evidence.

12. Risk appetite and PEP requirements

12.1. The risk appetite is determined by the Company according to the principles of proportionality and reasonableness and observing the context presented by the following risks:

a) the risks associated with the products and services offered, their volumes and complexity, including in different jurisdictions;
b) the risks of the customers consuming the products and services and the structure of the customer portfolio;
c) the risks of sales channels, incl. risks associated with outsourcing;
d) geographic risks, including presence in other countries or provision of services to cross-border customers from distance.

12.2. The Company's management board has determined that business relationships can be established with persons from a country outside the European Economic Area or with e-residents.

12.3. The relevant employee shall check whether the customer is a politically exposed person (PEP), a family member of a PEP or a person known to be a close associate with a PEP.

12.4. In order to allow a PEP to be the customer of ours, the following must be fulfilled:

a) An approval from our Company's management board for establishing a business relationship with that person.
b) Take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship.
c) Where a business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.

12.5. The relevant employee shall refuse to onboard the customer or, if an account is already opened, block the account and report to the Compliance Officer in case the relevant employee finds out that:

a) the customer is accessing the service from a high-risk country;
b) the customer is under sanctions from the European Union or the United Nations;
c) the customer is known to be accused with money laundering or terrorist financing.

13. International sanctions

13.1. The relevant employee shall check every customer on being subject to international sanctions. The check needs to be done during onboarding process and on a regular basis afterwards. If the relevant employee has doubts about the matching results and the customer in question, the relevant employee needs to consult with the Compliance Officer.

13.2. Upon instructions from the Compliance Officer, the relevant employee can request additional information from the customer to match the results.

13.3. The customer shall not be informed that he/she is screening under international sanctions' lists.

13.4. The relevant employee can check the list of persons under international sanctions following the link: https://www.politsei.ee/et/rahapesu/

13.5. The following information shall be recorded about each single check about the customer:

a) Check time;
b) Name of the relevant employee who made a check;
c) Check results;
d) Measures taken.

13.6. If the relevant employee identifies the customer who is subject to the international sanctions, the relevant employee shall inform the Compliance Officer. If the Compliance Officer agrees with the results, the Compliance Officer shall notify the management board.

14. Reporting procedure of suspicious and unusual transactions

14.1. If the relevant employee has a suspicion that he or she may be dealing with a suspicious or unusual transaction, the employee shall promptly report this to the Compliance Officer. In addition to the above-mentioned transaction and customer data, the Compliance Officer should also receive the reason for reporting and identification information about the customer.

14.2. The relevant employee is not allowed to notify the customer about the fact that the customer has been reported to the Compliance Officer.

14.3. In case of any suspicion, the relevant employee must notify the Compliance Officer by filling out the special notification form. The Compliance Officer must consider each report to determine whether it gives rise to grounds for knowledge or suspicion. Where such suspicion is determined, a suspicious transaction report made by the Compliance Officer shall be sent to the Financial Intelligence Unit.

14.4. The relevant employee must report to the Compliance Officer when he or she discovers any suspicious customer's behaviour related to money laundering, including, but not limited to cases where:

a) The customer makes transfers to other persons in different countries that do not conform to the person's usual activities;
b) The customer informs that the funds will be withdrawn by a third party acting on his/her behalf and on his/her account;
c) The customer's profile does not conform to the nature of the transaction being executed by him/her.

14.5. In case of suspicion of terrorist financing, the relevant employee must identify the risk related to the customer and report to the Compliance Officer if the risks related to a customer cannot be reasonably mitigated or explained.

14.6. The Company must report suspicious or unusual transactions to the Financial Intelligence Unit immediately, but not later than within two working days after identifying the activity or facts or after getting the suspicion.

14.7. The risks of terrorist financing include, but are not limited to:

a) The individual was born in a high-risk country;
b) The individual is a citizen of a high-risk country;
c) The individual has a place of residence in a high-risk country or the legal entity is incorporated in a high-risk country;
d) The natural person is associated with a legal person or another entity registered in a high-risk country.

15. A person in charge of the performance of the AML/CFT obligations

15.1. The designated management board member shall be in charge of the compliance with the MLTFPA and relevant guidelines.

15.2. The management board may appoint a Compliance Officer for performance of AML/CFT duties and obligations. The management board shall co-ordinate the appointment of the Compliance Officer with the FIU.

15.3. Compliance Officer is a person who acts as the contact person for the Financial Intelligence Unit ensuring the compliance with the measures put in place to prevent money laundering and terrorist financing at our Company.

15.4. The Compliance Officer needs to have the adequate education, professional suitability, abilities, personal qualities, experience and impeccable reputation required for performance of its duties.

15.5. Compliance Officer shall have the following duties:

a) Checking compliance with the money laundering prevention requirements in our Company and carrying out training for the employees.
b) Carrying out preliminary analysis of submitted reports about suspicious transactions and deciding whether or not to refer a report to the Financial Intelligence Unit.
c) Sending information to the Financial Intelligence Unit in the case of suspected money laundering and responding to queries and precepts made by the Financial Intelligence Unit.
d) Gathering information received from employees about suspicious and/or unusual actions, processing such information and keeping records pursuant to the prescribed procedure.

e) Prepares written overviews on compliance with money laundering and terrorist financing prevention requirements to the management board.
f) Notifying the management board in writing of any problems with compliance with these internal Rules of Procedural, guidelines and other legal acts and making periodic submission of written statements on compliance with the requirements arising from the MLTFPA.

15.6. Rights of the Compliance Officer:

a) Making proposals for amending these Rules of Procedure, AML policy, and any other policies of our Company that are related to anti-money laundering and the prevention of terrorist financing;
b) Monitoring the activities of the employees in pursuing the measures to prevent money laundering and terrorist financing.
c) Receiving data and information required for performance of the duties of the Compliance Officer.
d) Making proposals for re-organising the process of submission of notifications of suspicious and unusual transactions.
e) Receiving training in the field.

15.7. The Compliance Officer may send the information or data that have become known to him or her in connection with suspected money laundering only to:

a) The management board of the Company or to an employee especially appointed by the management board.
b) The Financial Intelligence Unit.
c) A preliminary investigating authority in connection with criminal proceedings;
d) The court on the basis of a court ruling or judgement.

15.8. In the event of a well-founded suspicion concerning money laundering or terrorist financing, the Compliance Officer shall promptly report it to the Financial Intelligence Unit.

15.9. A report shall be sent to the Financial Intelligence Unit using the web-based reporting form at https://www.politsei.ee/et/saada-teade. Copies of the documents that serve as the basis for a transaction, as well as the data or copies of the documents used as the basis for identifying a person, shall be enclosed with the filled-in reporting form.

15.10. The customer shall never be notified about any report sent about him or her to the Financial Intelligence Unit.

15.11. If the activities of a customer are not, in accordance with these Rules of Procedure, fully classifiable as activities which are to be reported to the Financial Intelligence Unit, any future activities of such customer shall be under increased scrutiny. The Financial Intelligence Unit shall be notified immediately if there is a well-founded suspicion about the behaviour of the customer.

15.12. No company, employee, the Compliance Officer or any other person acting on behalf of our Company shall be liable for any damage which may arise from non-completion or late completion of a transaction that is incurred by the customer because of suspicions about terrorist financing or money laundering that have been reported in good faith to the Financial Intelligence Unit.

15.13. Reporting to the Financial Intelligence Unit and sending relevant information shall not be deemed to be a violation of the duty of confidentiality laid down by law or a contract and no liability prescribed by legislation or a contract shall be attributed to those persons for disclosure of such relevant information.

16. Internal control rules

16.1. The Compliance Officer is responsible for checking the work done by the relevant employee.

16.2. The Compliance Officer shall check the work of the relevant employee on a quarterly basis in accordance with the following criteria:

a) the work of the relevant employee does not breach this Rules of procedure;
b) the relevant employee has done sufficient research on the customer;

c) the relevant employee has documented all the evidences about the customer;
d) the relevant employee has made a decision relaying on the evidences collected and documented.

16.3. The relevant employee may get a low-quality notification from the Compliance Officer if the relevant employee constantly breaches the criteria set forth in 16.2. In case the quality of the employee's work has not been improved after the first notification, this may lead to extraordinary termination.

17. Training for employees

17.1. The Compliance Officer or other expert in the field of anti-money laundering shall carry out the money laundering and terrorist financing prevention training for the employees of our Company.

17.2. The employees must be informed about the requirements for the prevention of money laundering and terrorist financing and the implementation of due diligence measures and reports on suspicion of money laundering. It includes:

a) the principles specified in the risk appetite of the company;
b) the risks arising from the activities of and services provided by the company;
c) the obligations stipulated in these rules of procedure;
d) the contemporary methods of committing money laundering and terrorist financing and specific typologies/cases, and the risks associated with them;
e) how to recognize actions related to possible money laundering or terrorist financing, and guidelines on how to act in such situations.

17.3. The Compliance Officer is responsible for carrying out regular training. Each relevant employee shall confirm their participation with their signature. It is recommended to organize trainings when necessary, but not less than once per year.

17.4. The Compliance Officer is obligated to provide instructions and an introduction training to all new relevant employees pursuant to the prescribed procedure following the signing of the employment contract no later than within one week after the commencement of employment by the relevant employee and to make the new relevant employee familiar with these Rules of Procedure against signature.

17.5. The Compliance Officer has the right to submit proposals to the management board concerning what trainings should be made.

18. Violation of duty to register information and keep records

18.1. Any violation of the duty to register information and to keep records as prescribed by these Rules of Procedure and in the Money Laundering and Terrorist Financing Prevention Act shall be disciplined in accordance with the law.

19. Outsourcing

19.1. Outsourcing of any obligation under these Rules of Procedure is allowed only upon respective resolution by the management board. Outsourcing is allowed only to a party that applies due diligence measures similar to those stipulated in these Rules of Procedure and the MLTFPA and provided the respective party is ready to be subject to supervision similar to one exercised over the Company in accordance with the MLTFPA.

19.2. To outsource an activity, the obliged entity enters into a written contract with the other person. The contract must ensure:

a) division of the rights and obligations associated with the outsourcing of the activity;
b) that the outsourcing of the activity does not impede the activities of the Company or performance of the obligations provided for in the law and guidelines;
c) that the other person performs all the obligations of the Company relating to the outsourcing of the activity;
d) that the outsourcing of the activity does not impede exercising supervision over the Company;

e) that the competent authority can exercise supervision over the person carrying out the outsourced activity;
f) the required level of knowledge and skills and the capacity of the person conducting the outsourced activity;
g) that the Company has the unrestricted right to inspect compliance by the person conducting the outsourced activity;
h) that documents and data gathered comply with the requirements arising from the law and relevant guidelines;
i) the right of the obliged entity to terminate the outsourcing contract with the other person, where necessary, if the latter has failed to perform the contractual obligations or has not performed them properly.

19.3. The Company or the relevant employee may rely on the data and documents gathered by a third-party if the Company or the relevant employee:

a) gathers from the third-party information on the identity of the person establishing the business relationship or making the transaction, their representative and the beneficial owner, as well as the purpose and nature of the business relationship or transaction;

b) has ensured that, where necessary, Company or the relevant employee is able to immediately obtain all the data and documents that were gathered by the third-party;

c) has established that the third-party is required to comply and actually complies with requirements equal to those established in the relevant law and is under or is prepared to be under state supervision regarding compliance with the requirements.

19.4. In the case of identification of person and verification of data using information technology means described in section 4, identification and data verification and the questionnaire can be carried out by a relevant employee, a partner of the Company or by an automated system.

20. Requests from the Financial Intelligence Unit

20.1. Upon the request of a supervision officer of the Financial Intelligence Unit all necessary documents and information shall be provided to the inspectors immediately.

21. Prevention of conflicts of interest

21.1. In order to identify and manage conflicts of interests, the Company:

a) established the risk appetite and risks arising from its activities;

b) avoids situations where the personal interests of owners, managers and employees and customers are in conflict with the interests of the Company;

c) asks the employees and managers to provide data about their economic interests that may originate a conflict of interests. The Company regularly updates these declarations of economic interests;

d) identifies and analyses whether the persons who lead a customer to the Company has a conflict of interests between the Company and the customer. The measure to manage such a conflict of interests may be to avoid establishing such business relationship.

22. Amendments of these Rules of Procedure

22.1. These Rules of Procedure may be amended by resolution of the management board based on a majority vote in accordance with the articles of association of the Company.

---oOo---