RULES OF PROCEDURE
FOR PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING
AND
COMPLIANCE WITH INTERNATIONAL SANCTIONS

Established by the decision of the management board of CRYPTOGRAFIC OÜ, registry code 14843601 (hereinafter Provider of service) on16.01.2022.

_____

1. General provisions

1.1. These rules of procedure for prevention of money laundering and terrorist financing, and compliance with international sanctions (hereinafter **Rules**) lay down requirements for screening the Clients (as defined in section 2.7) in order to prevent entering into deals involving suspected Money Laundering and Terrorist Financing, and to ensure identification and reporting of such.

1.2. The obligation to observe the Rules rests with Management Board members and employees of the Provider of service, including temporary staff, agents of the Provider of service who initiate or establish Business Relationship (as defined in section 2.6) (hereinafter all together called the **Representative**). Every Representative must confirm awareness of the Rules with the signature.

1.3. The Rules are primarily based on the regulations of Money Laundering and Terrorist Financing Prevention Act (hereinafter **the Act**) and International Sanctions Act (hereinafter **ISA**).

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

1.5. 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 (hereinafter **FIU**) at https://www2.politsei.ee/en/organisatsioon/rahapesu-andmeburoo/.

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

2. Definitions

2.1. Money Laundering – is a set of activities with the property derived from criminal activity or property obtained instead of such property with the purpose to:

i. conceal or disguise the true nature, source, location, disposition, movement, right of ownership or other rights related to such property;

ii. convert, transfer, acquire, possess or use such property for the purpose of concealing or disguising the illicit origin of property or of assisting a person who is involved in criminal activity to evade the legal consequences of his or her action;

iii. participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to subsections 2.1.i and 2.1.ii.

2.2. Terrorist Financing – acts of financing of terrorism as defined in § 237^3 of the Penal Code of Estonia.

2.3. International Sanctions – list of non-military measures decided by the European Union, the United Nations, another international organisation or the government of the Republic of Estonia and aimed to maintain or restore peace, prevent conflicts and restore international security, support and reinforce democracy, follow the rule of law, human rights and international law and achieve other objectives of the common foreign and security policy of the European Union.

2.4. Compliance Officer or CO – representative appointed by the Management Board responsible for the effectiveness of the Rules, conducting compliance over the adherence to the Rules and serving as contact person of the FIU.

2.5. FIU - Financial Intelligence Unit of the Police and Border Guard Board of Estonia.

2.6. Business Relationship – a relationship of the Provider of service established in its economic and professional activities with the Client.

2.7. Client – a natural or legal person, who uses services of the Provider of service.

2.8. Beneficial Owner – is a natural person, who:

i. Taking advantage of his influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed taking advantage of his influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favour or on whose account a transaction or act, action, operation or step is made.

ii. Ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means. Direct ownership is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company. Indirect ownership is a manner of exercising control whereby a company which is under the control of a natural person holds or multiple companies which are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

iii. Holds the position of a senior managing official, if, after all possible means of identification have been exhausted, the person specified in clause ii cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner.

iv. In the case of a trust, civil law partnership, community or legal arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such associations': settlor or person who has handed over property to the asset pool, trustee or manager or possessor of the property, person ensuring and controlling the preservation of property, where such person has been appointed, or the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.

2.9. Politically Exposed Person or PEP - is a natural person who is or who has been entrusted with prominent public functions including a head of state, head of government, minister and deputy or assistant minister; 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; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a state-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials.

2.9.1. The provisions set out above also include positions in the European Union and in other international organizations.

2.9.2. A family member of a person performing prominent public functions is the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a parent of a politically exposed person.

2.9.3. A close associate of a person performing prominent public functions is 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; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

2.10. Local Politically Exposed Person or local PEP – a natural person, provided in section 2.9, who performs or has performed prominent public functions in Estonia, a contracting state of the European Economic Area or in an institution of European Union.

2.11. Provider of service – CRYPTOGRAFIC OÜ.

2.12. Virtual currency exchange service is a service within the framework of which a person exchanges a virtual currency for money or money for a virtual currency or one virtual currency for another.

2.13. Virtual currency wallet service is a service within the framework of which encrypted keys of customers are created or stored, which can be used for the purpose of storing, storing and transmitting virtual currencies

2.14. Virtual currency transfer service is a service that allows, at least in part, an electronic transaction through a virtual currency service provider on behalf of the originator to transfer the recipient's currency to a virtual currency wallet or account, the recipient uses the same service provider;

2.15. Virtual currency - a value represented in the digital form, which is digitally transferable, preservable or tradable and which persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4(25) of Directive (EU) 2015/2366 of the European Parliament and of the

Council on payment services in the internal market or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same directive.

2.16. Management Board or MB – management board of the Provider of service. Member of the MB, as appointed by relevant MB decision, is responsible for implementation of the Rules.

2.17.

3. Prohibition to carry out cash transactions or cash payments

The company will not accept operations (in wallet or exchange) in cash, understanding this within the meaning of article 2, section 2, of Regulation (EC) no 1889/2005 of the European Parliament and of the Council on controls of cash entry or abandon the Community (OJ L 309 of 25.11.2005, pp. 9-12).

4. Prohibition to carry out cash with Shell Banks

4.1. The company will not accept transactions in which the origin or destination of the funds involves a shell bank.

4.2. Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country.

5. Description of activities of the Provider of service

5.1. The Provider of service is the provider of a virtual currency wallet service in the framework of which the Provider of service provides hot and cold wallets for clients where funds are transferred and can be used for the purpose of keeping and storing virtual currencies.

5.2. The Provider of a service of exchanging a virtual currency against a fiat currency, and vice versa.

5.3. The Provider of a service of exchanging a virtual currency against a virtual currency.

5.4. The Provider of service is a subject to authorisation by the FIU.

6. Compliance Officer

6.1. The MB shall appoint a CO whose principal tasks are to:

- 6.1.1. monitor the compliance of the Rules with the relevant laws and compliance of the activity of the Representatives with the procedures established by the Rules;
- 6.1.2. compile and keep updated the data regarding countries with low tax risk, high and low risk of Money Laundering and Terrorist Financing and economical activities with great exposure to Money Laundering and Terrorist Financing;
- 6.1.3. carry out training, instruct and update the Representatives on matters pertaining to procedures for prevention of Money Laundering and Terrorist Financing;
- 6.1.4. report to the MB once a year (or more frequently, if necessary) on compliance with the Rules, and on circumstances with a suspicion of Money Laundering or Terrorist Financing;
- 6.1.5. collect, process and analyse the data received from the Representatives or Clients concerning suspicious and unusual activities;
- 6.1.6. collaborate with and report to the FIU on events of suspected Money Laundering or Terrorist Financing, and respond to enquiries of the FIU;
- 6.1.7. make proposals on remedying any deficiencies identified in the course of checks.

6.2. The CO must meet all the requirements, prescribed by the Act, and appointment of the CO shall be co-ordinated with the FIU. If, as a result of a background check carried out by the FIU, it becomes evident that the CO's credibility is under suspicion due to their previous acts or omissions, the Provider of service may extraordinarily terminate the CO's employment contract due to the loss of credibility.

6.3. Tasks of the CO can be performed by a department, therefore provisions of section 4.2 will apply accordingly.

7. Client admission policy.

CRYPTOGRAFIC has approved a CLIENT ADMISSION POLICY, adopting reinforced precautions with respect to those clients who present a risk higher than the average risk.

By virtue of the foregoing, the following clients will not be admitted:

• Those who do not provide all the information requested in a reasonable period of time in order to comply with the obligations imposed by Money Laundering and Terrorist Financing Prevention Act (Rahapesu ja terrorismi rahastamise tõkestamise seadus) .
• Those who are known to have been convicted of a crime of tax fraud, drug trafficking, money laundering and human trafficking.
• People who appear on the current official blacklists, without express authorization from the Prevention of Money Laundering.
• People for whom some information is available that may be related to criminal activities.
• People about whom there are suspicions about the origin of the funds and / or the actual owner of the contract.
• People who have businesses whose nature makes it impossible to verify the legitimacy of the activities or the origin of the funds.
• Legal persons whose ownership or control structure could not be determined.
• People or entities that reside in a territory with a risk level higher than 4 (see annex I) without the authorization of the board of directors
• Any other category determined by the board of directors.

Clients will be questioned about their present or past status as a person with public responsibility.

In the event that such a condition is suspected or verified, all due diligence measures will be observed with special care in order to ascertain the origin of its assets and the funds to be allocated to the operation.

No commercial relations will be established with any client that carries out illegal or prohibited activities by law, or that, despite not being prohibited in their country of origin, is contrary to the Spanish legal system.

8. Application of due diligence measures

8.1. The Service Provider shall determine and take due diligence (hereinafter DD) measures using results of conducted risk assessment (see Section 10), and provisions of national risk assessment, published on the web-page of the Ministry of Finance of Estonia.

8.2. The Representatives shall pay special attention to circumstances that refer to Money Laundering or Terrorist Financing.

8.3. The service provider shall not accept a payment made to an payee with an anonymous prepaid card if all the following conditions are not met:

1) the prepaid card is not rechargeable and the amount of money held electronically does not exceed 150 euros;
2) the prepaid card is used only for the purchase of goods or services;
3) the prepaid card cannot be financed with anonymous e-money;
4) the issuer of the prepaid card monitors transactions or business relationships sufficiently to be able to identify unusual or suspicious transactions;
5) the amount of the payment does not exceed 50 euros.

8.4. The Service provider shall identify both the payer and the payee in respect of each transfer of funds which complies with Regulation (EU) No 2015/847 of the European Parliament and of the Council on

information on remittances and repealing Regulation (EC) No 1781/2006 (OJ L 141, 05.06.2015, p. 1–18), with a financial obligation from at least EUR 1000, regardless of whether the financial obligation is met in a single transaction or in several interconnected transactions over a period of up to one month.

8.5. Currency exchange services may be provided without identifying the person participating in the transaction if the value of the amount exchanged for cash in a single transaction or related transactions does not exceed 1000 euros.

8.6. The Service Provider shall not provide services which can be used without identifying the person participating in the transaction and verifying the information submitted, except in the cases specified in these rules.

8.7. The Service Provider shall open an account and maintain the account in the name of the account holder.

8.8. Depending on the level of the risk of the Client and depending on the fact whether the Business Relationship is an existing one or it is about to be established, the Provider of service shall apply either normal DD measures (see Section 6), simplified DD measures (see Section 8) or enhanced DD measures (see Section 9). The Provider of service shall also apply continuous DD measures to ensure ongoing monitoring of Business Relationships (see Sections 5.7-5.10).

8.9. DD measures shall include the following procedures:

i. Identifying the Client and verifying its identity using reliable, independent sources, documents or data, including e-identifying;
ii. Identifying and verifying of the representative of the Client and the right of representation;
iii. Identifying the Client's Beneficial Owner;
iv. Assessing and, as appropriate, obtaining information on the purpose of the Business Relationship;
v. Conducting ongoing DD on the Client's business to ensure the Provider of service's knowledge of the Client and its source of funds is correct;
vi. Obtaining information whether the Client is a PEP or PEP's family member or PEP's close associate.

8.10. The Provider of service shall establish the source of wealth of the Client, where appropriate.

8.11. To comply with the DD obligation, the Representatives shall have the right and obligation to:

i. request appropriate identity documents to identify the Client and its representatives;
ii. request documents and information regarding the activities of the Client and legal origin of funds;
iii. request information about Beneficial Owners of a legal person;
iv. screen the risk profile of the Client, select the appropriate DD measures, assess the risk whether the Client is or may become involved in Money Laundering or Terrorist Financing;
v. re-identify the Client or the representative of the Client, if there are any doubts regarding the correctness of the information received in the course of initial identification;

8.12. The objective of the continuously applied DD measures is to ensure on-going monitoring of Clients. Conducting ongoing monitoring of the Business Relationship includes:

i. Keeping up-to-date the documents, data or information, obtained during taking DD measures;
ii. Paying particular attention Client's conduction, leading to criminal activity or Money Laundering or Terrorist Financing;
iii. Paying particular attention to the Business Relationship, if the Client is from or the seat of a Client being a legal person is located in a third country, which is included in the list of risk countries (see Exhibit 1).

8.13. Annual review of a Client being a legal entity is carried out regularly once a year. Updated data shall be recorded in the Provider of service's Client database.

8.14. The Representative updates the data of a Client, who is either a legal person or a natural person, i.e. takes appropriate DD measures every time when:

i. the Client addresses the Provider of service with the request to amend a long-term contract during the term of its validity;

ii. upon identification and verification of the information there is reason to suspect that the documents or data gathered earlier are insufficient, have changed or are incorrect. In this case, the Representative may conduct a face-to-face meeting with the Client;

iii. the Provider of service has learned through third persons or the media that the activities or data of the Client have changed significantly.

8.15. The Representative shall evaluate the substance and the purpose of the Client's activities, in order to establish the possible links with Money Laundering or Terrorist Financing. The evaluation should result in an understanding about the purpose of the Business Relationship for the Client, the nature of the Client's business, the risk levels of the Client and, if necessary, the sources of funds.

8.16. In order to establish his identity, the Service Provider must collect at least the person's telephone number and e-mail address as contact details.

8.17. The Service Provider is required to apply at least the due diligence measures provided for these section in the case of a virtual currency exchange or transfer service.

8.18. Upon entering into a virtual currency exchange or transfer transaction, the originator's virtual currency service provider shall identify the identity of each customer in accordance with these provisions and collect at least the following information concerning the originator:

1) in the case of a natural person, the name, unique identifier of the transaction, identifier of the payment account or virtual currency wallet, the name and number of the identity document and the personal identification code or date of birth, place of residence and address of residence;

2) in the case of a legal person, the name, unique identifier of the transaction, identifier of the payment account or virtual currency wallet, registry code, in its absence the relevant identification of the country of location (combination of numbers or letters equivalent to the registration number) and address of location.

8.19. When performing a virtual currency exchange or transfer transaction, the virtual currency service provider shall collect data on the unique identifier of the transaction for the virtual currency or transfer recipient and the payment account or virtual currency wallet identifier if the payment account or virtual currency wallet identifier is used for the transaction. For the purposes of this section, a unique identifier of a transaction is a combination of letters, numbers or symbols assigned by the virtual currency service provider in accordance with the system protocol used to trace the transaction from the originator to the transferee.

8.20. The originator of a virtual currency service provider shall immediately and securely transmit the information specified in this section to the recipient's virtual currency service provider. The transmission of data may be arranged together with the transmission of a set of payment orders to the payee's virtual currency service provider or to the payee's credit or financial institution.

8.21. If the recipient's virtual currency wallet does not have a virtual currency service provider or the recipient's service provider is unable to receive or process data, the obligation described in of this section is deemed to be fulfilled if both the originator and the recipient's virtual currency service providers monitor transactions and , using the technological solution provided for that purpose, and if the virtual currency service provider of the originator of the transaction maintains the data specified in this section in a manner that allows them to be submitted immediately upon request by the supervisory or investigative authority.

9. Normal due diligence measures

9.1. The Provider of service shall conduct normal DD in the following cases:

i. Upon establishing a new Business Relationship;

ii. In the event of insufficiency or suspected incorrectness of the documents or information gathered previously in the course of carrying out DD measures;

9.2. In the course of conducting normal DD measures, the Representative shall apply the measures of DD as provided for in section 5.4.

9.3. No new Business Relationship can be formed, if the Client, in spite of the respective request, has failed to present documents and appropriate information required to conduct DD, or if based on the presented documents, the Representative suspects Money Laundering or Terrorist Financing.

9.4. If in spite of the respective request an existing Client has failed to present during the contract period documents and appropriate information required to conduct DD, such behaviour constitutes material breach of contract that shall be reported by the Representative to the CO, and in such case the contract(s) concluded with the Client shall be cancelled and the Business Relationship shall be terminated as soon as feasible[1].

9.5. The Provider of service shall not enter into Business Relationships with anonymous Clients.

10. Identification of a person

10.1. Upon implementing DD measures the following person shall be identified:

i. Client – a natural or legal person;
ii. Representative of the Client – an individual who is authorized to act on behalf of the Client;
iii. Beneficial Owner of the Client;
iv. PEP – if the PEP is the Client or a person connected with the Client (see Section 2.9).

10.2. Upon establishing the relationship with the Client, the Provider of service shall identify and verify the Client while being present at the same place as the Client or by using information technology means.

10.3. For identification of a Client and verification of the identity of a Client by using information technology means, the Provider of service shall use:

10.3.1. a document issued by the Republic of Estonia for the purpose of digital identification;

10.3.2. another electronic identification system within the meaning of the Regulation (EU) No 910/2014 of the European Parliament and of the Council[2]. If the Client is a foreign national, the identity document issued by the competent authority of the foreign country is also used simultaneously.

10.4. In case of identification of a Client and verification of the identity of a Client by using information technology means the Provider of service shall additionally obtain data from a reliable and independent source, e.g. identity documents databases.

10.5. A person can be identified and the data can be checked by using IT tools if:

1) the Business Relationship is established with an e-resident or a Person who is from a country that is not a contracting state of the European Economic Area or whose residence or location is in such a country and if due diligence measures are not applied by being at the same place as the person or their representative.

2) the Business Relationship is established with a person who is from a contracting state of the European Economic Area or whose residence or location is in such a country and whose total outgoing payments related to the Transaction in one calendar month from at least, in case of a natural person, EUR 15,000 and, in case of a legal person, EUR 25,000, and if due diligence measures are not applied by being at the same place as the person or their representative.

10.6. To identify a person and verify data by means of IT tools, a document meant for digital verification of identity issued by the Republic of Estonia or other e-identification system of high reliability is used. If the person is a foreign national, an identity document issued by a competent foreign authority must also be used for the identification and verification of data.

10.6.1. A document intended for digital identification issued by the Republic of Estonia or another electronic identification device with a high level of trust specified in a regulation established on the basis of this section shall be used for identification and verification of data by means of information technology.

10.6.2. If a person is a citizen of a foreign state, in addition to the information specified in this section, an identity document issued by a competent authority of a foreign state shall be used simultaneously for identification and verification of information.

---

[1] The termination of the long-term contract or contract without the term must foresee the Provider of service's right to terminate the contract extraordinarily without observing the period of pre-notice in case the Client does not provide requested identification or verification documents (in due time)

[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1510127223064&uri=CELEX:32014R0910

10.6.3. In addition, information from a reliable and independent source shall be used to establish identity and verify data. A credit institution and a financial institution have the right to use the identification data entered in the database of identity documents for the purpose of establishing identity and verifying data.

10.6.4. The technical requirements and procedure for the identification and verification of data by means of information technology means shall be established by a regulation of the minister responsible for the field, in particular the Technical requirements and procedures for identification and verification of data by means of information technology of Minister of Finance Adopted on 23.05.2018.

10.7. In non-face-to-face operations, the identity of the natural person or the representative of the legal person who wants to establish a business relationship and occasionally conclude a transaction by means of information technology will be verified. you must use a document intended for the digital identification of a person and issued on the basis of the Identity Documents Act or other highly trusted electronic identification system, which has been added to the list published in the Official Journal of the European Union on the basis of Article 9 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and an information technology medium with a camera, microphone, the hardware and software required for digital identification and an adequate quality Internet connection.

10.8. Accepted documents for non-Estonian citizens will require any local identity document verified through an EIDAS certified tool; a digital identity card issued by Estonia (if the person has one) and a travel document. After the identification of a person and the verification of the person's identity, systems will be implemented that allow facial recognition and the comparison of biometric data. Information from a reliable and independent source is also used for the identification and verification of data. To identify an e-resident and verify their data, the Employee has the right to use the identification data entered in the database of identity documents.

10.9. Identification of a Client being a natural person and a representative of a Client who is a legal person

10.9.1. Upon establishing a Business Relationship, identification takes place, above all, during a face-to-face meeting or by using information technology means.

10.9.2. The Rules must be considered when dealing with the documents that can be used to identify the Client or its representative and the requirements established for them (see Section 7.10). If it is not possible to obtain original documents for identification of a Client, request documents certified or authenticated by a notary public or authenticated officially for verification of the identity of the natural person, or use data obtained from other reliable and independent sources (including electronical identification) on condition that information is obtained from at least two different sources. For transactions less than 10,000 euros, the apostille and notarization will not be necessary as long as the verification is carried out through the resources and software approved by CRYPTOGRAFIC.

10.9.3. Verification must be made whether or not such person is a PEP (see Section 7.9).

10.9.4. A new Client and, if necessary, an existing Client shall confirm the correctness of the submitted information and data by signing the Client data registration sheet (see Form 1).

10.9.5. The Service Provider shall establish the identity of a customer and, where appropriate, his or her representative and preserve the following information concerning the person and, where appropriate, his or her representative:

1) name;

2) personal identification code, in the absence thereof, date of birth and residence or seat;

3) information concerning the identification and control of the right of representation and the extent thereof, and if the right of representation does not arise from law, the name of the document on which the right of representation is based, the date of issue and the name of the issuer.

10.9.6. The Service Provider shall verify the accuracy of the information specified iy using information from a reliable and independent source (See Webshield Section).

10.9.7. The Service Provider shall establish the identity of a natural person on the basis of the following documents:

1) a document specified in subsection 2 (2) of the Identity Documents Act;

2) a valid travel document issued in a foreign state;

3) a driving license which complies with the conditions provided for in subsection 4 (1) of the Identity Documents Act or

4) in the case of a person under 7 years of age, a birth certificate specified in § 30 of the Civil Status Act.

10.9.8. If the original document specified in subsection (3) of this section cannot be seen, a notarised or notarised or officially certified document specified in subsection (3) or other information from a reliable and independent source may be used to verify identity, including e-identification and e-transaction trust services, using at least two different sources to verify the data.

10.9.9. The requirement to use two different sources specified in this section need not be applied to a client with limited active legal capacity on whose behalf a business relationship is established or a transaction is entered into by his or her representative.

10.10. Identification of a Client being a legal person

10.10.1. To identify a Client who is a legal person, the Representative shall take the following actions:

i. Check the information concerning a legal person by accessing the relevant electronic databases (e-commercial register/ e-äriregister and European Business Register)To consult the Public Registers within the European Union Area, it will be accessed from the following link:
https://e-justice.europa.eu/content_business_registers_in_member_states-106-en.do?init=true (English version)
https://e-justice.europa.eu/content_business_registers_in_member_states-106-et.do?init=true
(Estonian version)

ii. If it is not possible to obtain an original extract from the register or the respective data, request documents (extract from the relevant registry, certificate of registration or equivalent document) certified or authenticated by a notary public or authenticated officially for verification of the identity of the legal person, or use data obtained from other reliable and independent sources (including electronical identification) on condition that information is obtained from at least two different sources;

iii. Ask the representative of a foreign legal person to present an identity documents and a document evidencing of his/her power of attorney, which has been notarised or authenticated pursuant to an equal procedure and legalised or authenticated by a certificate substituting for legalisation (apostille), unless otherwise prescribed by an international agreement;

iv. On the basis of the information received from the representative of the foreign legal person, control whether or not the legal person could be linked with a PEP (see Section 7.9);

v. If the seat of a Client being a legal person is located in a third country, which is included in the list of risk countries (see Exhibit 1), report this to the CO, who shall decide the additional measures to be applied to identifying and background checking of the person.

10.10.2. The document presented for identification of a legal person shall set out at least the following:

i. business name, registry code (number), date of registration, seat and address;

ii. names and authorisations of members of the Management Board or the head of branch or the other relevant body.

10.10.3. A legal representative of a new Client (subsequently as required) shall confirm the correctness of the submitted information and data by signing the Client data registration sheet (see Form 1).

10.11. Consequences of insufficient identification of a Client

10.11.1. Should the Representative establish that the identification of a Client is insufficient the Representative shall:

i. Promptly apply the enhanced DD measures pursuant to the Rules;
ii. Notify the CO of the failure to implement normal DD in a timely manner;
iii. Assess the risk profile of the Client and notify CO and/or MB for the purposes of the provisions in Section 12.3.

10.12. Identification of the Beneficial Owner of the Client

10.12.1. Registration and assessment of the Beneficial Owner(s) of a legal person is mandatory.

10.12.2. There is no need to identify the Beneficial Owners of a Client/company whose securities have been accepted for trading on a regulated securities market.

10.12.3. In order to establish the Beneficial Owner, the Representative shall take the following actions:

i. Gather information about the ownership and control structure of the Client on the basis of information provided in pre-contractual negotiations or obtained from another reliable and independent source;
ii. In situations, where no single person holds the interest or ascertained level of control to the extent of no less than 25 per cent (see Section 2.9), apply the principle of proportionality to establishing the circle of beneficiaries, which means asking information about persons, who control the operations of the legal person, or otherwise exercise dominant influence over the same;
iii. If the documents used to identify a legal person, or other submitted documents do not clearly identify the Beneficial Owners, record the respective information (i.e. whether the legal person is a part of a group, and the identifiable ownership and management structure of the group) on the basis of the statements made by the representative of the legal person, or a written document under the hand of the representative;
iv. To verify the presented information, make enquiries to the respective registers, and request an annual report or another appropriate document to be presented.
v. If no natural person is identifiable who ultimately owns or exerts control over a Client and all other means of identification are exhausted, the senior managing official(s) might be considered to be the Beneficial Owner(s).
vi. Pay attention to companies established in low tax rate regions (see Exhibit 1).

10.12.4. While establishing the Beneficial Owner, it is possible to rely on information received in a format reproducible in writing from a credit institution registered in the Estonian commercial register or from the branch of a foreign credit institution, or from a credit institution that has been registered or whose place of business is in a contracting state of the European Economic Area.

10.13. Identification of Politically Exposed Person

10.13.1. The Representative shall implement the following measures to establish whether or not a person is a PEP:

i. asking the Client to provide necessary information;
ii. making an enquiry or checking the data on websites of the respective supervisory authorities or institutions of the country of location of the Client;
iii. making an inquiry to the special PEP databases.

10.13.2. The matter of whether to establish a Business Relationships with a PEP, or a person associated with him or her, and the DD measures applied to such person shall be decided by the MB.

10.13.3. If a Business Relationship has been established with a Client, and the Client or its Beneficial Owner subsequently turns out to be or becomes a PEP, CO and MB shall be notified of that.

10.13.4. In order to establish a Business Relationship with a PEP or a company connected with that person, it is necessary to:

i. take enhanced DD measures (see Section 9);
ii. establish the source of wealth of this person;
iii. monitor the Business Relationship on a continual basis at least once per 6 months.

10.13.5. DD measures, mentioned in Section 7.9.4 might be not applicable regarding local PEPs, if there are no relevant circumstances, leading to the higher risks.

10.13.6. Respective remark must be made in the Provider of service's database of Clients on documents of such person in the form of notation "Politically Exposed Person".

10.14. Documents that can be used for identification

10.14.1. In case of Clients being natural persons and the representatives of Clients, the following documents can be used for identification[3]:

i. Personal ID card (whether ID card, e-resident card or residence permit card);
ii. Passport or diplomatic passport;
iii. Travel document issued in a foreign country;
iv. Driving licence (if it has name, facial image, signature and personal code or date of birth of holder on it).

10.14.2. The Representative shall make a copy of the page of identity document which contains personal data and photo.

10.14.3. In addition to an identity document, the representative of a Client shall submit a document in the required format certifying the right of representation.

10.14.4. Legal person and its passive legal capacity shall be identified and verified on the basis of the following documents:

i. in case of legal persons registered in Estonia and branches of foreign companies registered in Estonia, the identification shall be conducted on the basis of an extract of a registry card of commercial register;
ii. foreign legal persons shall be identified on the basis of an extract of the relevant register or a transcript of the registration certificate or an equal document, which has been issued by competent authority or body not earlier that six months before submission thereof.

10.14.5. If not original documents are used for identification, the Representative shall control and verify data by using at least two reliable and independent sources.

11. Simplified due diligence measures

11.1. Simplified DD measures may be taken, if the Client is:

i. A company listed on a regulated market that is subject to disclosure requirements consistent with European Union law;
ii. a legal person governed by public law founded in Estonia;
iii. a governmental authority or another authority performing public functions in Estonia or a contracting state of the European Economic Area;
iv. an authority of the European Union;
v. a credit institution or a financial institution, acting on behalf of itself, located in a contracting state of the European Economic Area or in a third country (see Exhibit 1), which in the country of location is subject to equal requirements and the performance of which is subject to state supervision.

12. Enhanced due diligence measures

[3] About documents to be used for identification: https://www.politsei.ee/et/organisatsioon/rahapesu/kasulikku/isikusamasuse-tuvastamine.dot
Authenticity of personal ID documents can be checked here: http://www.consilium.europa.eu/prado/ET/prado-start-page.html (14.02.2017) or here: https://www.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/

12.1. Enhanced DD measures must be taken in cases where the risk level of the Client is higher.
12.2. The Representative shall establish the Client's risk profile and determine the risk category in accordance with the Rules. The risk category may be altered during the course of the Business Relationship, taking into consideration the changes in data gathered.
12.3. The Representative, who upon entering into a Business Relationship with a new Client, detects that there is at least one of the following high-risk characteristics present in respect of a Client, shall consult with and report to the CO, and shall take the DD measures set out in the Rules.
12.4. The Representative shall apply enhanced DD measures in the following situations:
12.4.1. when suspicion arises regarding truthfulness of the provided data and/or of authenticity of the identification documents regarding the Client or its Beneficial Owners;
12.4.2. the Client is a PEP (excluding local PEPs, if there are no relevant circumstances, leading to the higher risks);
12.4.3. the Client is from or the seat of a Client being a legal person is located in a third country, which is included in the list of risk countries (see Exhibit 1);
12.4.4. in case of companies that have nominee shareholders or shares in bearer form;
12.4.5. in a situation with higher risk of Money Laundering and terrorists financing as described in Sections 9.1 and 9.3.
12.5. Enhanced DD measures shall include at least one the following measures in addition to normal DD measures as established in Section 5.4:
12.5.1. Identification and verification of a Client on the basis of additional documents, data or information, which originates from a reliable and independent source;
12.5.2. Identification and verification of a Client while being present at the same place;
12.5.3. Asking the identification or verification documents to be notarised or officially authenticated;
12.5.4. Obtaining additional information on the purpose and nature of the Business Relationship and verification from a reliable and independent source;
12.5.5. the making of the first payment related to a transaction via an account that has been opened in the name of the Client in a credit institution registered or having its place of business in a contracting state of 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;
12.5.6. 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;
12.6. Reassessment of a risk profile of a Client not later than 6 months after establishment of Business Relationship.
12.7. After taking enhanced DD measures, the MB shall decide whether to establish or continue the Business Relationship with the Client in respect of whom the enhanced DD measures were taken.
12.8. If a Client who, by the date of entry into a contract, has not performed any prominent public functions for at least a year, and such person is deemed to pose no further risk specific to PEP, this Client is not considered as the PEP, therefore application of enhanced DD measures is not required.
12.9. The Representative may not apply enhanced DD measures stipulated in section 9.5 to local PEP, if there are no other circumstances leading to the higher risk.

13. Additional due diligence measures

13.1. The service Provider chooses additional due diligence measures in order to manage and mitigate an established risk of money laundering and terrorist financing that is higher than usual.
13.2. To perform the duties provided for in subsection 1 of this section, the obliged entity may, among other things, apply one or several of the following due diligence measures:
1) verification of information additionally submitted upon identification of the person based on additional documents, data or information originating from a credible and independent source;

2) 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;

3) 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;

4) 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;

5) the making of the first payment related to a transaction via an account that has been opened in the name of the person or customer participating in the transaction in a credit institution registered or having its place of business in a contracting state of 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) the application of due diligence measures regarding the person or their representative while being at the same place as the person or their representative.

13.3. Upon application of enhanced due diligence measures, the obliged entity must apply the monitoring of a business relationship more frequently than usually, including reassess the customer's risk profile not later than six months after the establishment of the business relationship.

13.4. In addition to the measures provided for in this section, the measures provided for in § 41 of the Money Laundering and Terrorism Financial Prevention Act also apply to a politically exposed person, their family member or a person known to be their close associate. Where there is a factor that refers to a lower risk regarding the aforementioned person, the application of the aforementioned measures is required only where there is a factor referring to a higher risk.

14. Enhanced due diligence measures applied to transaction made with natural and legal persons operating in high-risk third country

14.1. Where the Service Provider comes in contact with a high-risk third country via a person participating in a transaction made in the obliged entity's economic or professional activities, via a person participating in an official operation, via a person using an official service or via a customer, the Service Provider applies the following due diligence measures:

1) gathering additional information about the customer and its beneficial owner;

2) gathering additional information on the planned substance of the business relationship;

3) gathering information on the origin of the funds and wealth of the customer and its beneficial owner;

4) gathering information on the underlying reasons of planned or executed transactions;

5) receiving permission from the senior management to establish or continue a business relationship;

6) improving the monitoring of a business relationship by increasing the number and frequency of the applied control measures and by choosing transaction indicators or transaction patterns that are additionally verified;

14.2. In addition the Service Provider may demand that a customer make a payment from an account held in the customer's name in a credit institution of a contracting state of the European Economic Area or in a third country that implements requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council.

14.3. In addition to subsection the Service Provider applies one or several of the following due diligence measures:

1) winding up its branch or representation in a high-risk third country;

2) carrying out a special audit in a subsidiary or branch of the credit institution or financial institution in a high-risk third country;

3) assessing and, where necessary, terminating a correspondent relationship with an obliged entity of a high-risk third country.

15. Transactions with politically exposed person

15.1. In a situation where the person participating in a transaction made in economic or professional activities, the person participating in an official operation, the person using an official service, the customer

or their beneficial owner is a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person, the obliged entity applies the following due diligence measures in addition to the due diligence measures of these Rules:

1) obtains approval from the senior management to establish or continue a business relationship with the person;

2) applies measures to establish the origin of the wealth of the person and the sources of the funds that are used in the business relationship or upon making occasional transactions;

3) monitors the business relationship in an enhanced manner.

15.2. Where a politically exposed person no longer performs important public functions placed upon them, the Service Provider must at least within 12 months take into account the risks that remain related to the person and apply relevant and risk sensitivity-based measures as long as it is certain that the risks characteristic of politically exposed persons no longer exist in the case of the person.

16. Prohibition on making transactions and establishing business relationships

16.1. The Service Provider is prohibited from establishing a business relationship or enabling the conclusion or completion of a transaction occasionally or within the framework of a business relationship if at least one of the following circumstances exists:

1) he or she fails to perform due diligence measures required by this Act;

2) he or she has a suspicion that it is money laundering or terrorist financing.

16.2. The Service Provider is prohibited from establishing a business relationship or entering into a transaction with a person whose capital is more than 10 per cent of the bearer's shares or other bearer securities.

16.3. The Service Provider is prohibited from executing a customer's payment order or making funds available if he or she fails to perform the obligation provided for in subsection 19 (4) or subsection 25 (1 1) of this Act .

16.4. If he customer's refusal to provide information or documents necessary for the implementation of due diligence the Money Laundering Information concerning a suspicious transaction pursuant to the procedure provided for in § 49 of the Money Laundering and Financial Terrorism Prevention Act. The business relationship is deemed to be terminated by submitting a notice of termination to the customer, after which the obligated person completely restricts the provision of the service to the customer.

16.5. The Service provider is prohibited from executing a customer's payment order or making funds or virtual currency available if he fails to perform the obligations provided in these rules or in Money Laundering and Terrorist Financing Prevention Act

16.6. The provider has established, in accordance with these internal rules of procedure established based on the risk analysis, in which case the virtual currency will be returned to the originator and in which case it will not be made available to the recipient. The service provider shall consider the completeness and sufficiency of the data of the originator and recipient of a transaction when determining the existence of a higher risk and considering notifying the Financial Intelligence Unit of a suspicious transaction pursuant to § 49 of Money Laundering and Terrorist Financing Prevention Act.

16.7. An agreement which violates the prohibition provided for in subsections (1) - (3) of this section is void.

16.8. The provisions of this section do not apply if the Service Provider has notified the FIU of the establishment of a business relationship, transaction or attempted transaction and received specific instructions from the FIU to continue the business relationship, establishment or transaction.

17. Risk assessment

17.1. The Representative will establish a risk profile of a Client based on information gathered under the Rules.

17.2. The Provider of service applies the following risk categories:

i. Normal risk (the risk level is normal, there are no high risk characteristics present);

ii. High risk, which is subcategorized as High risk I and High risk II.

17.3. For every Client, who does not fall into the "normal risk" category, the Representative shall record the Client's risk category in the Provider of service's database of Clients and on the documents as "High risk I" or "High risk II". Only the CO shall have the right to change the risk category recorded for a Client.

17.4. Assessment of risk profile of natural persons

17.4.1. When establishing the risk category of a Client being a natural person, the country of residence of the Client, the region where the Client operates, and status of PEP shall be taken into account.

17.4.2. If there are several characteristics of the category "High risk I" present, or if, in addition to the characteristics of "High risk I", at least one of the "High risk II" characteristics is present, the Client shall be determined to be falling into the category "High risk II".

17.4.3. Characteristics of high risk in the case of a natural person, and the appropriate DD measures:

High risk category I	DD measures
The actual place of residence or employment or business of a Client is in a country, which is included in the list of risk countries (see Exhibit 1), or the Client is an official citizen/resident of such country.	Ask the Client to provide additional information about the purpose of establishing the Business Relationship and his/her economic activities. Ask the Client to provide additional information about its links with the said foreign state.
The Client is a person associated with a PEP.	The decision is taken by the MB.
The Client is a local PEP.	Conduct an internet search about the Client. Ask additional information and documents, which prove the legal origin of Client's assets. If there are no other circumstances leading to the higher risk and the MB approves, it is not required to apply enhanced DD measures stipulated in section 10.7.

High risk category II	DD measures
The Client is a PEP or a person associated with him or her.	Conduct an internet search about the Client. Ask additional information and documents, which prove the legal origin of Client's assets.
There is information that the Client is suspected to be or to have been linked with a financial offence or other suspicious activities.	Check information about International Sanctions (see also Section 15)[4] or ask guidance from the CO. Ask additional information and documents, which prove the legal origin of the Client's assets.
The Client is a non-resident individual, whose place of residence or activities is in a country, which is listed in the list of risk countries (see Exhibit 1).	Ask the Client to provide additional documents to identify the Client and, if possible, check the Client's data vis-à-vis the previously presented documents and information. Verify and compare the data submitted by the Client against the additional documents, data or information, which originates from a reliable and independent source.

17.5. Assessment of risk profile of legal persons

[4] For search regarding financial sanctions imposed against a person please refer to: https://www.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/

17.5.1. When establishing the risk category of a legal person, assessment shall be based on the country of location of the legal person, its area of activity, the transparency of ownership structure and the management.

17.5.2. If there are several characteristics of the category "High risk I", or if, in addition to the characteristics of "High risk I", at least one of the "High risk II" characteristics is present, the Client shall be determined to be falling into the category "High risk II".

17.5.3. Characteristics of high risk in the case of a legal person, and the appropriate DD measures

High risk category I	DD measures
The Client is a legal person registered in the European Economic Area or in Switzerland, whose area of activity is associated with enhanced money-laundering risk (see Exhibit 1).	Ask the Client to provide additional documents to identify it and, if possible, check the Client's data vis-à-vis the previously presented documents and information. Verify and compare the data submitted by the Client against the additional documents or information, which originates from a reliable and independent source.
The Client is situated in a country, which is listed in the list of risk countries (see Exhibit 1, Annex I and Annex II).	Ask the Client to provide additional information about its links with the said foreign state. Ask for additional information about the purpose of establishing the Business Relationship.
The legal person is a non-profit association, trust, civil law partnership or another contractual legal arrangement, whose activities and liability are insufficiently regulated by law, and the legality of financing of which is not easy to screen.	Check the authenticity of the presented documents and verify the accuracy of the data. Ask for help from the CO. Ask the Client to provide information about relationships with other credit or financing institutions, and the opinion of the respective credit or financing institution. Ask additional information and documents, which prove the legal origin of the Client's assets.
The representative or the Beneficial Owner of a legal person is a local PEP or his or her family member.	Ask the Client to provide additional information about the need and purpose of establishing the Business Relationship. Ask the Client to provide information about relationships with other credit or financing institutions, and the opinion of the respective credit or financing institution about the Client. Conduct an internet search about the Client, being a legal person, and its Beneficial Owner. Ask additional information and documents, which prove the legal origin of the Client's assets. If there are no other circumstances leading to the higher risk and the MB approves, it is not required to apply enhanced DD measures stipulated in section 10.7.

High risk category II	DD measures
The representative or the Beneficial Owner of a legal person is a PEP or his or her family member.	Ask the Client to provide additional information about the need and purpose of establishing the Business Relationship. Ask the Client to provide information about relationships with other credit or financing institutions, and the opinion of the respective credit or financing institution about the Client. Conduct an internet search about the Client, being a legal person, and its Beneficial Owner.

	Ask additional information and documents, which prove the legal origin of the Client's assets.
There is information that the person is suspected to be or to have been linked with a financial offence or other suspicious activities.	Check information about International Sanctions (see also Section 15).[5] or ask guidance from the CO. Ask additional information and documents, which prove the legal origin of the Client's assets.
A legal person registered outside the European Economic Area, whose field of business is associated with a high risk of Money Laundering (see Exhibit 1). A legal person registered outside the European Economic Area, who is operating outside the country of its registered location. A legal person is operating or is registered in a low tax rate country (see Exhibit 1) or the place of residence, place of registration of the legal person, its owners or Beneficial Owners, or the territory of business of the legal person is situated in a country listed in the list of risk countries (see Exhibit 1).	Ask the Client to provide additional information about its links with the said foreign state. Ask for additional information about the purpose of establishing the Business Relationship. Verify and compare the data submitted by Client against the additional documents, data or information, which originates from a reliable and independent source (if obtaining such information is possible). Ask additional information and documents, which prove the legal origin of the Client's assets.

17.6. The above listed DD measures can be combined, as appropriate, in respect to other listed or non-listed risks.

18. Webshield

18.1. All clients must be checked before entering into the business relationship through the webshield tool.

18.2. This tool has the following functionalities:

- Portfolio Cross-Check
- InvestiGate reveals previously unknown relationships: Entities clustered around directors, UBOs or even addresses.
- Underwriting Checklist
- InvestiGate's optional underwriting checklist lets you tick of the right boxes and highlights the tasks still on the table.
- Virtual Address Detection
- Gain access to our ever-growing virtual presence database. An interactive map ensures you know where a merchant really resides.
- Business Classification
- Review the current business-related recommendations by the card schemes and modify crawling routines for special business types.
- Website Auto-Compliance
- Verify if merchants properly inform customers about their terms and conditions or correctly disclose their contact details.

[5] See footnote 3

- Audit Trail
- Audit Trail ensures every decision can be traced back to an individual and guarantees accountability throughout the underwriting process.
- SiteAlert
- SiteAlert notifies you about any hit on our verified crowdsourced warning list or blacklist.
- License Verification
- License Verification automatically matches the merchant's name against the associated whitelists and lets you upload the relevant license.
- Timeline View
- Knowing the precise history of events allows you to reconstruct compliance issues, spot recurring patterns in merchant behaviour.

18.3. All employees will take training courses to learn how the webshield tool works.

19. Registration and storage of data

19.1. The Representative shall ensure that Client data are registered in the Provider of service's Client database within the required scope.

19.2. Registration of data of a Client who is natural person

19.3. The following obtained data shall be recorded in the Provider of service's information system:

i. Name, personal ID code or, in the absence of the latter, date of birth and the address of the person's permanent place of residence and other places of residence;
ii. the name and number of the document used for identification and verification of the identity of the person, its date of issue and the name of the issuing authority;
iii. occupation, profession or area of activity – establish the area of activity (occupation) and the status of the person (trader, employee, student, pensioner);
iv. If the Client is a natural person, the Representative shall record information about whether the person is performing or has performed prominent public functions, or is a close associate or family member of the person performing prominent public functions;
v. Citizenship and the country of tax residency;
vi. the origin of assets.

19.4. In case of a representative, the following info shall be recorded:

i. same as provided for in pints i-ii of Section 11.2.1;
ii. the name of the document used for establishing and verification of the right of representation, the date of issue and the name or name of the issuing party.

19.5. If the Business Relationship is established by the Client or the representative with the use of the ID card or other e-identification system, the data of the document used for identification is saved automatically in the digital signature. If identification takes place at a face-to-face meeting with the Client, the data of the document used for identification is recorded on the copy of the identification document.

19.6. <u>Registration of data of a Client who is a legal person</u>

19.6.1. The following information on the Client being a legal person shall be recorded:

i. Name, legal form, registry code, address, date of registration and activity locations;
ii. information concerning means of communication and contact person(s);
iii. names of the members of the management board or an equivalent governing body, and their powers to represent the Client, and whether any of them is a PEP;
iv. information about the Beneficial Owners;
v. Field(s) of activity (i.e. the NACE codes);
vi. name and number of the document used for identification and verification of the identity, its date of issue and the name of the issuing authority;
vii. country of tax residency of the legal person (VAT number);
viii. date of registration of the legal person in the Provider of service's database;
ix. purpose of the Business Relationship;

x. origin of assets (normal business operations/other);

19.6.2. The following information about the Beneficial Owner shall be recorded:

i. Name, personal ID code or, in the absence of the latter, date of birth and place of residence;

ii. type of control over the enterprise (e.g. shareholder);

iii. is the person a PEP;

iv. information about the representative as set forth under 11.2.2.

19.6.3. If the Business Relationship is established by the representative of the Client with the use of the ID card or other e-identification system, the data of the document used for identification is saved automatically in the digital signature. If identification takes place at a face-to-face meeting with the representative of the Client, the data of the document used for identification is recorded on the copy of the identification document.

19.6.4. Information from the B-card, i.e. the legal representatives of the Client being a legal person stated on the B-card, shall be recorded on the Client data registration sheet or the contract concluded with the Client.

19.7. The Representative shall record all the data regarding:

19.7.1. Provider of service's decision to refuse establishment Business Relationship. The Representative shall record all the data, if, as a result of taking DD measures, a person refuses to establish the Business Relationship.

19.7.2. Impossibility to take DD measures due to information technology means;

19.7.3. Termination of the business relationship, as a result of impossibility to take DD measures;

19.8. Storage of Data

19.8.1. The respective data is stored in a written format and/or in a format reproducible in writing and, if required, it shall be accessible by all appropriate staff of the Provider of service (MB, Representatives, marketing, CO etc).

19.8.2. The originals or copies of the documents and information related to the performance of the obligations provided in these rules for establishing a Business Relationship, shall be stored for at

19.8.3. The data of the document prescribed for the digital identification of a Client, information on making an electronic query to the identity documents database, and the audio and video recording of the procedure of identifying the person and verifying the person's identity shall be stored at least five (5) years following the termination of the Business Relationship.

19.8.4. Also to be stored:

i. manner, time and place of submitting or updating of data and documents;

ii. name and position of Representative who has established the identity, checked or updated the data.

20. Monitoring

In addition, a continuous monitoring of the business relationship must be carried out, checking that the operations carried out throughout said relationship coincide with the knowledge that it has of the client, its activity and origin of its funds. For this, the client's information must be kept updated, as well as their documents.

The Director of Compliance will carry out a report on the ongoing relationship of the business relationship that will be executed on a monthly, quarterly, semi-annual or annual basis according to the assessment of your risk appetite and the following structure will be followed:

- EXAMINATION OF THE INITIAL RISKS
- DEVELOPED OPERATIONS
- ANALYZED INFORMATION
- ACTIONS MADE
- RISK ASSESSMENT

- EVALUATION OF THE ORIGIN OF INTERRUPTING OR DECLINING THE BUSINESS RELATIONSHIP
- EVALUATION ON THE ORIGIN OF COMMUNICATION TO THE SEPBLAC
- OBSERVATIONS

In order to control the client's operations and control their level of risk, REALISTO has implemented a system, through its "MOTO" application, in order to detect IP coincidences of the originators of the transactions and assigning a level of risk to the transaction according to the territory of origin / destination of the funds, thresholds according to amounts and a comparison of the average-maximum ticket information declared by the client or that appears in their usual operations.

For this, the operations department will include the data related to the activity declared by the client in the client registration form (average ticket / maximum / monthly and annual volume) and will be updated periodically according to the client's trajectory.

The accounting department will report to the money laundering prevention department the operations that the MOTO application marks as suspicious.

The software will mark as suspicious those operations whose origin or geographical destination are classified as high-risk territories, exceed the average ticket thresholds declared or usual for the client.
Likewise, the compliance / money laundering prevention department will include in the risk analysis report of the continuing business relationship the valuation and results of the client's operations together with the analysis of returns (refunds) and chargebacks (chargebacks) with the purpose of conducting an overall analysis.

If it is necessary or there are doubts about the operation detected, the client will be required to provide justification for them and additional documentation will be required to support them (tickets, invoices, order sheets, order tracking ...).

In the event that the justification and information is not sufficient, is incomplete or is contradictory with the result of the investigations carried out, the AML Officer of the entity will be transferred to make a decision on the continuation of the business relationship and the measures to adopt.

If the result shows sufficient evidence of money laundering, the provisions in the communication section of this manual will be followed.

21. Reporting

21.1. Notification of the CO

21.1.1. Any circumstances identified in the Business Relationship are unusual or suspicious or there are characteristics which point to Money Laundering, Terrorist Financing, or an attempt of the same the Representative shall promptly notify the CO.

21.1.2. The CO shall analyse and forward the respective information to the MB.

21.2. Notification of FIU

21.2.1. Before reporting any transaction connected with suspected Money Laundering or Terrorist Financing to the FIU, the CO shall analyse the content of the information received, considering the Client's current area of activity and other known information.

21.2.2. The CO shall decide whether to forward the information to the FIU and the MB shall decide whether to terminate the Business Relationship.

21.2.3. The CO shall make a notation "AML" behind the name of the Client in the Provider of service's Client database or on the documents, and shall notify the FIU promptly, but not later than within 2 business days after discovering any activities or circumstances or arising of suspicion, using the

respective web-form for notifying the FIU. Copies of the documents as set forth by guidelines of FIU or further requested by FIU shall be appended to the notice.

21.2.4. The FIU shall be notified of any suspicious and unusual transactions where, including such where the financial obligation exceeding 32 000 euros or an equivalent amount in another currency is performed in cash, regardless of whether the transaction is made in a single payment or several related payments.

21.2.5. The CO shall store in a format reproducible in writing any reports received from the Representatives about suspicious circumstances, as well as all information gathered to analyse such notices, as well as other linked documents and notices to be forwarded to the FIU, along with the time of forwarding the notice, and the information about the Representatives who forwarded the same.

21.2.6. The Client who is reported to the FIU as being suspicious, may not be informed of the same.

21.2.7. It is also prohibited to inform any third persons, including other Representatives, of the fact that information has been reported to the FIU, and the content of the reported information, except for the MB/CO.

21.3. Termination of the Business Relationship with a Client in the event of suspected Money Laundering and Terrorist Financing

21.3.1. Pursuant to law, the Provider of service is obliged to extraordinarily and unilaterally terminate the Business Relationship without observing the advance notification period, if:

i. The Client fails to present upon identification or upon updating the previously gathered data or the taking of DD measures, true, full and accurate information, or

ii. The Client or a person associated with the Client does not present data and documents evidencing of the lawfulness of the economic activities of the Client, or

iii. the Provider of service suspects for any other reasons that the Client or the person associated with the Client is involved in Money Laundering or Terrorist Financing, or

iv. the documents and data submitted by the Client do not dispel the Provider of service's suspicions about the Client's possible links with Money Laundering or Terrorist Financing.

21.3.2. The decision on terminating the Business Relationship shall be taken by the Management Board, considering also the proposal of the CO.

21.3.3. The Client shall be notified of the termination of Business Relationship in writing, provided that it is consistent with Section 12.2.7. Notation about the cancellation of the Business Relationship shall be made in the Provider of service's Client database or documentation, and a note "AML" shall be added to the Client's data, provided that it is consistent with Section 12.2.8.

21.4. Indemnification of the Representatives

21.4.1. The Provider of service and its Representatives shall not, upon performance of the obligations arising from the Rules, be liable for damage arising from failure to carry out any transactions (by the due date) if the damage was caused to the persons in connection with notification of the FIU of the suspicion of Money Laundering or Terrorist Financing in good faith, or for damage caused to a Client or in connection with the cancellation of a Business Relationship on the basis provided in Section 12.3.

21.4.2. Fulfilment of the notification obligation by the Representative acting in good faith, and reporting the appropriate information shall not be deemed breach of the confidentiality obligation imposed by the law or the contract, and no liability stemming from the legislation or the contract shall be imposed upon the person who has performed the notification obligation.

22. Implementation of International Sanctions

22.1. The Provider of service is required to implement International Sanctions in force.

22.2. Representatives shall draw special attention to all its Clients (present and new), to the activities of the Clients and to the facts which refer to the possibility that the Client is a subject to International Sanctions.

Control and verification of possibly imposed International Sanctions shall be conducted by the Representatives as part of DD measures applied to the Clients in accordance with these Rules.

22.3. The Representatives who have doubts or who know that a Client is subject to International Sanctions, shall immediately notify the CO. In case of doubt, if the CO finds it appropriate, the Representative shall ask the Client to provide additional information that may help to identify whether he/she is subject to International Sanctions or not.

22.4. The CO shall be responsible for the implementation of International Sanctions.

22.4.1. The CO shall:

i. regularly follow the webpage of FIU (https://www.politsei.ee/et/rahapesu/) and immediately take measures provided for in the act on the imposition or implementation of International Sanctions; Likewise, other European and international sources will be consulted depending on the country of origin of the client and the databases of the United Nations, EU, OFAC and Interpol through the following links:

SANCTIONS LISTS

☒UNITED NATIONS SANCTIONS (UN)
https://www.un.org/sc/suborg/es/sanctions/un-sc-consolidated-list

☐ AUSTRALIAN SANCTIONS
https://dfat.gov.au/international-relations/security/sanctions/Pages/consolidated-list.aspx

☐ BUREAU OF INDUSTRY AND SECURITY (US)
https://www.bis.doc.gov/

☒ EU FINANCIAL SANCTIONS (*con contraseña)
https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions

☐ OFFICE OF THE SUPERINTENDENT OF FINANCIAL INSTITUTIONS (CANADA)
http://www.osfi-bsif.gc.ca/Eng/fi-if/amlc-clrpc/atf-fat/Pages/default.aspx

☒ OFAC - SPECIALLY DESIGNATED NATIONALS (SDN)
https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

☒ UK FINANCIAL SANCTIONS (HMT)
https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

☒ US CONSOLIDATED SANCTIONS
https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx

☐ DEPARTMENT OF STATE, AECA DEBARRED LIST (US)
https://www.state.gov/r/pa/prs/ps/2018/04/281189.htm

☐ DEPARTMENT OF STATE, NONPROLIFERATION SANCTIONS (US)
https://www.state.gov/t/isn/c15231.htm

☒ INTERPOL WANTED LIST
https://www.interpol.int/notice/search/wanted

☐ SANCTIONS LIST FINALCIAL INTELIGENCE OF INDIA (IND)
https://fiuindia.gov.in/files/misc/unscsanction.html

☐ SWITZERLAND SANCTION LIST – SECO
https://www.seco.admin.ch/seco/en/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/sanktionen-embargos/sanktionsmassnahmen/suche_sanktionsadressaten.html

ii. upon entry into force of an act on the imposition or implementation of International Sanctions, the amendment, repeal or expiry thereof, immediately check whether any of the Clients is

subject to International Sanctions with regard to whom the financial sanction is imposed, amended or terminated;

iii. if an act on the imposition or implementation of International Sanctions is repealed, expires or is amended in such a manner that the implementation of International Sanctions with regard to the subject of International Sanctions is terminated wholly or partially, terminate the implementation of the measure to the extent provided for in the act on the imposition or application of International Sanctions;

iv. keep an updated record of subjects of International Sanctions and submit this information to the Representatives in the form that allows to use this information in the course of their activity;

v. provide training to the Representatives that allows them to establish independently the subjects of International Sanctions;

vi. assist the Representatives if they have doubt or knowledge that a Client is a subject to International Sanctions;

vii. supervise the application of the Rules regarding the implementation of International Sanctions by the Representatives;

viii. review and keep updated the Rules regarding the implementation of International Sanctions

ix. notify FIU of Clients who are subject to International Sanctions or in part of whom the CO, the Representatives have doubts;

x. keep record of made checks, notifications submitted to FIU and applied measures in part of detected subjects to International Sanctions.

22.4.2. When making checks on Clients as to detect whether they are subject to International Sanctions, the following information shall be recorded and preserved for five years:

i. Time of inspection;

ii. Name of person who carried out inspection;

iii. Results of inspection;

iv. Measures taken.

22.4.3. If in the course of the check, it shall be detected that a Client or a person who used to be a Client is subject to International Sanctions, the CO shall notify the Representatives who dealt with this Client, the Management Board and FIU. The notification shall be submitted at least in the way that allows its reproduction in writing.

22.4.4. The Client who is subject to International Sanctions and about whom the notification is made, shall not be informed of the notification.

22.4.5. Application of special measures and sanctions on the Client who is detected to be subject to International Sanctions should be authorized by FIU.

22.4.6. When making checks of Clients, the possible distorting factors in personal information (i.e. way of written reproduction of name etc.) must be kept in mind.

23. Questionnaire

In all client incorporation (onboarding) processes, it will be necessary to fill in a client identification questionnaire.

Said identification questionnaire will be used to determine the residential address of a natural person, the profile of the activity, the area of activity, the purpose and nature of the establishment of a commercial relationship, the connection of the economic or family interests of the person with Estonia, the estimated transaction volumes expected to be made, the beneficial owner, whether the person is a politically exposed person and other important information.

In the case of legal persons, it will serve to identify the registration code, the location and the places of operation, including branches located in foreign countries, the entity's legal form, legal capacity, legal and contractual representatives, beneficiaries real and, if applicable, if the beneficial owner is a politically exposed person, economic connections with Estonia, contracting states of the European Economic Area

and third countries, major trading partners, the activity profile of the legal entity, main areas of activity and Secondary, purpose and nature of establishing a business relationship and other important information.

24. Interview

A real-time interview will be carried out to collect and verify the information and data necessary for the determination of the customer profile, during which the The Service Provider employee will ask questions the questions in order to corroborate the information provided in the questionnaire and expand information if necessary, emphasizing the volume of transactions that will be carry out, the purpose or nature of the business relationship, the description of business activity, based on the results of the identification questionnaire.

The interview will be carried out individually so that no other person may attend the interested party or his representative for the duration of the interview, unless the natural person or the legal representative of the legal entity needs assistance from another person to eliminate any technical problems when conducting the interview.

The employee will evaluate their conclusions from the interview in writing. It will include in them the client's reaction during the interview, the reliability of the information and data obtained and the compliance with the information and data obtained with other procedures, and will record their opinion and the circumstances that are the basis of it

25. Client-Activity Risk Report

17.1 The AML compliance officer must evaluate all the documentation provided during the onboarding process, the results of the interview and the questionnaire, as well as the results of the checks and verifications carried out. For this purpose, a report on “client risk and activity will be prepared, in which the client risk, geographic risk, the risk of the activity carried out by it, transactional risk and channel risk will be holistically assessed. The structure of the report will consist of the following parts:

I.- Customer Profile
II.- Client Risk
III.- Activity Risk
IV.- Geographical Risk
V.- Transactional Risk
VI.- Canal Risk
VII.- Observations
VIII.- Conclusions

17.2 The report will end with the final assessment of the risk according to the assessment algorithms approved by the entity and its rating (low, medium, medium high, high or very high)

17.3 The report will include the AML compliance officer's assessment of whether the client is fit, unfit or should be subject to assessment by the Board of Directors either because there are indications of Money Laundering or because their risk level exceeds the thresholds. allowed. It will also include the periodicity of monitoring the client's transactions according to their risk level (weekly, monthly, quarterly, semi-annually) and any additional measures that may be necessary

26. Employee evaluation procedure

26.1. The Service Provider will demand high ethical standards in the hiring of employees, managers and agents. For this reason, no employee or manager accused or convicted of Money Laundering or corruption will be hired.

26.2. Persons who carry out AML-related duties shall be against with a minimum of 2 years experience in similar functions and shall be against with adequate training. For the performance of the duties of compliance officer or Internal Auditor the minimum required experience will be 5 years.

26.3. The entity will adopt the appropriate measures so that its employees are aware of the requirements derived from the AML act, International Sanctions act, FATF-FACT Recommendations, European Regulations

and Supervisory Authorities, as well as other relevant associations in the fight against money laundering. ACAMS , ACFE.

26.4. These measures will include the duly accredited participation of employees in specific permanent training courses aimed at detecting operations that may be related to money laundering or terrorist financing and instructing them on how to proceed in such cases. The training actions will be the subject of an annual plan that, designed according to the risks of the business sector of the and of the various departments, will be approved by the administrative body.

26.5. The company will try to train its employees annually with at least two training courses in the prevention of Money Laundering and analysis of suspicious operations / risk analysis.

26.6. A record will be kept of all the training actions taught. This record will contain:

• Date and place of the call and duration of each course. • Personnel to whom the training is given.
• List of attendees indicating name and trainer.
• Course content.
• Support material used.
• Documentation delivered to each attendee.

26.7. In the case of new labor incorporations, said employees must be summoned as quickly as possible to carry out the training course, in order to achieve adequate training to detect the operations related to money laundering and give know how to proceed in such cases.

26.8. The knowledge acquired by the participants will also be evaluated by means of a questionnaire / evaluation test, recording it, as well as the calls, assistants and documentation used.

27. Internal audit and amendment of the Rules

27.1. Compliance with the Rules shall be inspected at least once a year by the CO, whose job duties are set out in Section 4.1.

27.2. The report on the results of the inspection concerning the compliance with the measures for prevention of Money Laundering and Terrorist Financing shall set out the following information:

i. time of the inspection;
ii. name and position of the person conducting the inspection;
iii. purpose and description of the inspection;
iv. analysis of the inspection results, or the conclusions drawn on the basis of the inspection.

27.3. If the inspection reveals any deficiencies in the Rules or their implementation, the report shall set out the measures to be applied to remedy the deficiencies, as well as the respective time schedule and the time of a follow-up inspection.

27.4. If a follow-up inspection is carried out, the results of the follow-up inspection shall be added to the inspection report, which shall state the list of measures to remedy any deficiencies discovered in the course of the follow-up inspection, and the time actually spent on remedying the same.

27.5. The inspection report shall be presented to the MB, who shall decide on taking measures to remedy any deficiencies discovered.

28. Internal control and storage of data

28.1. The service provider shall implement adequate internal control measures covering all levels of management and activities of the virtual currency service provider.

28.2. The supervisory board of the service provider shall appoint an internal auditor to perform the functions of the internal audit unit. The requirements and legal bases for the activities of a certified internal auditor in the Auditing Act apply to the internal auditor. The internal auditor shall not perform any duties which give rise to or may give rise to a conflict of interests.

28.3. The task of the internal auditor is to verify the compliance of the activities of the virtual currency service provider and its managers and employees with legislation, precepts of the Financial Intelligence Unit,

decisions of management bodies, internal rules, agreements entered into by the virtual currency service provider and good practice.

28.4. The service provider shall ensure that the internal auditor has all the rights and working conditions necessary for the performance of his or her duties, including the right to receive explanations and information from the managers and employees of the virtual currency service provider.

28.5. The internal auditor is required to immediately forward in writing to the managers of the virtual currency service provider and the Money Laundering Information Bureau information which has become known to him or her concerning the virtual currency service provider and which indicates violations or damage to the interests of clients.

28.6. The service provider shall keep the information provided for in this Act unchanged and available to the Financial Intelligence Unit for five years as of the termination of the business relationship with the customer.

28.7. The service provider shall preserve documents which set out the rights and obligations of the virtual currency service provider and the customer under the service provision agreement or the conditions under which the service is provided to the customer for as long as the contractual relationship with the customer lasts unless a longer term is provided for in this Act and other legislation.

29. Risk appetite assessments

29.1. CRYPTOGRAPHIC conducts a risk appetite analysis according to a series of indicators. These Criteria will apply to both the Wallet and Exchange services.by exchanging FIAT to Crypto, Crypto to FIAT and Crypto to Crypto. In these last services and following the "travel rule" included in the FATF Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers(https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf) appetite assessment Customer risk will also apply to the counterparty, whether it is the originator or the beneficiary of the transaction.

29.2. Risk appetite is understood as the set of risk levels and types of risks of the entity that it is willing to assume in the development of its activity and achieve its strategic objectives; and has been approved by the Board of Directors of CRYPTOGRAFIC.

29.3. The analysis will identify and assess the risks of CRYPTOGRAPHIC by types of customers, countries or geographic areas, products, services, operations, and distribution channels, taking into account variables such as the purpose of the business relationship, the level of customer assets, the volume of operations and the regularity or duration of the business relationship.

29.4. The risk analysis will be reviewed annually and, in any case, when a significant change is verified that could influence the risk profile. Likewise, it will be mandatory to carry out and document a specific risk analysis prior to the launch of a new product, the provision of a new service, the use of a new distribution channel or the use of a new technology by THE SERVICE PROVIDER, applying appropriate measures to manage and mitigate the risks identified in the analysis.

For the evaluation of the client risk, it will be considered if he is a person of public responsibility, if he acts alone or through a representative or intermediary, as well as other criteria such as his age, nationality and residence. In the case of legal persons, these same considerations will be considered for their beneficial owners and administrators, and the registered office will also be taken into account, if this coincides with the place of residence of the administrator and that of the bank branch with which it operates, if they have a complex structure or if they are duly registered in a public registry, among others.The risk parameterization based on these criteria will be prepared by the Compliance Officer and reviewed and approved annually at least by the Board of Directors of CRYPTOGRAPHIC.

29.5. Geographic Risk. These criteria will be applied to assess the country risk of both the origin of the client and its representatives or final beneficiaries, as well as to assess the origin and destination of the funds.

The evaluation, valuation and parameterization criteria will be prepared by the Compliance and Prevention of Money Laundering Officer and approved by the Board of Directors.

The following country factors have been considered in the currently approved guidelines:

- If they are considered third countries with strategic deficiencies identified by Decision of the European Commission in accordance with the provisions of article 9 of Directive (EU) 2015/849 of the European Parliament and of the Council, of May 20, 2015, with:

• the legal and institutional framework of the third country in the fight against money laundering and the financing of terrorism, and in particular:

o criminalization of money laundering and financing of terrorism,

o ii) the due diligence measures with respect to the client,

o iii) document retention requirements, and

o iv) requirements for reporting suspicious transactions.

• The powers and procedures of the competent authorities of third countries for the purpose of combating money laundering and financing of terrorism

• The effectiveness with which the system for combating money laundering and the financing of terrorism makes it possible to deal with the risks of the third country with respect to money laundering or the financing of terrorism.

- If they are considered countries, territories or jurisdictions that do not have adequate systems for the prevention of money laundering and the financing of terrorism.
- If they are considered Countries, territories or jurisdictions subject to sanctions, embargoes or similar measures approved by the European Union, the United Nations or other international organizations.
- If they are considered Countries, territories or jurisdictions that present significant levels of corruption or other criminal activities.
- If they are considered Countries, territories or jurisdictions in which financing or support for terrorist activities is provided.
- If they are considered Countries, territories or jurisdictions that have a significant offshore financial sector ("off-shore" centers).
- If they are considered Countries, territories or jurisdictions that are considered tax havens.
- According to your Geographic Region: Europe / Asia-Pacific / CEMEA / Latin America and the Caribbean / North America
- If they belong to the EU, Euro Zone, Schengen Zone and European Economic Area
- If they belong to the FATF-FAFT or another equivalent supranational organization (MONEYVAL / APG / CFAFT / EAG / ESAAMLG / GABAC / MENAFAFT / GIABA)
- The Corruption Perceptions Index rating published by Transparency International.

29.6. Activity Risk

To calculate the activity risk, will serve those activities that entail a greater risk of money laundering and, in particular, a risk level will be assigned based on their Merchant Category Code (MCC) with a rating of 1 to 5 with the corresponding risk rating: low , medium, medium high, high and very high.

The risk assessment will give a value from 1 to 5 with the corresponding risk rating: low, medium, medium high, high and very high.

This evaluation will be contrasted with software tools from external providers and IT and will be used to complement and reinforce the qualification carried out in accordance with the aforementioned parameters.

The report will end with the final risk assessment (scale 1-5) according to the assessment algorithms approved by the entity and its rating (low, medium, medium high, high or very high).

The report will include the evaluation of the compliance/prevention of Money Laundering officer on whether the client is suitable, not suitable or should be subject to evaluation by the Board of Directors, either because there are indications of Money Laundering or because their level of risk exceeds the permitted thresholds. It will also include the periodicity of the follow-up of the client's transactions according to their level of risk (monthly, quarterly, semi-annually or annually) and the additional measures that are necessary.

_____

For higher risk businesses relationships with national PEPs and PEPs from foreign organizations, the service Provider will take consistent additional measures such as the identification of the source of wealth and the source of funds when relevant.

29.7. Scale

29.7.1. CRYPTOGRAPHIC has a scale for assessing the customer's risk appetite or the counterparty, in the case of Exchange Services.

29.7.2. The score assigned to each client on a scale of 1-5 (including decimals) is the result of the sum of the categories of client risk, geographical risk, activity risk, channel risk and transactional risk. The sum of the values is not equal, but its percentage estimate when reflecting the result is the result of an algorithm approved by the entity itself according to the relevance assigned to each category. This algorithm will be reviewed annually or when the criteria considered are modified.

29.7.3. For the assessment of the geographical risk of the client, or the national risk of its administrators or beneficial owners, indicators such as the Region (Europe, Asia Pacific, CEME, AL/C) have been taken into account if it belongs to the EU , European Union Euro zone , Schengen Zone, if it is a cooperating, supervised or high territory according to the FATF, if it belongs to other supranational organizations such as APG, CFAT, MONEYVAL, EAG, GABAC, ESAAMLG, GAFILAT, GIABA or MENAFAFT. They will also be considered if they belong to a territory considered or included in black and gray lists as tax havens in Spain, Europe or the OECD and if they are countries subject to sanctions or considered sponsors of terrorism. The Corruption Perception Index published by Transparency International will also be considered.

29.7.4. For the risk of activity, the Merchants Category Codes will be considered based on Visa and Mastercad Card Systems assigned a scale value of 1-5.

29.7.5. For the channel risk, a scale value of 1-5 has been assigned depending on whether the transaction is carried out via credit card, bank transfer, through a service provider virtual currency (VASP) or a financial institution, P2P transaction. Likewise, the geographical area of the originator and the beneficiary of the transaction will also be considered.

29.7.6. CRYPTOGRAPHIC will only accept income, payment, distribution, movement, or transmission of fiduciary and virtual currencies through credit or prepaid cards, national or international transfers and P2P transactions.

29.7.7. For transactional risk, it will be assessed on a scale of 1-5 according to the amount of operation.
The tranches and scorings considered for transactional risk are as follows:
<€1000: Risk 1
1000-9999: Risk 2
10,000-14,900: Risk 3
15,000 – 100,000: Risk 4
> 100,000 :Risk 5

29.7.8. Analysis of the risk appetite of the Virtual Currency Service Provider of the counterparty, agents or other mediators that market the services offered by CRYPTOGRAFIC OÜ.

29.7.9. Will be taken into account for risk appetite assessment of the Virtual Currency Service Provider of the counterparty, agents or other mediators the following sources, resources and indicators: the AML/CFT laws and regulations of the country of origin or the country address, the geographic risk criteria of the country, public databases of legal decisions and/or regulatory actions or execution, annual reports that have been filed on a stock exchange, reports or other information published by international organizations that measure the compliance and What address ML/TF risks (including FATF, FSRB, BCBS, IMF and World Bank), lists issued by the FATF in the context of its International Cooperation of the Review Group process, reputable newspapers, magazines or other source electronic media, third-party databases, assessment of regulator and supervisor to which the Virtual Currency Service Provider of the country in which it has obtained the license is subject.

***

Form 1

Client Data

Updated:	Risk category

Client data sheet ('know your customer)

Name, address, etc.	Name	
	Personal code/Date of birth/Registry code	
	Address/Location	
	Citizenship (in case of natural person)	
	Occupation, area of activity	
	Name and date of issuance of document used for identification (in case of natural person and representative of legal person)	
	Name and number of the document used for identification and verification of the identity of a foreign legal person	
	Postal code and city	
	The country of tax residency	
	Area of activity (in case of legal person)	
	E-mail	Telephone
	Contact person and e-mail	Telephone
	Have the securities of the company been accepted for trading on a regulated securities market? (in case of legal person) NO YES, if Yes, then on which securities market?	

Beneficial Owner (in case of legal person)	Record the Beneficial Owners: *A Beneficial Owner is a natural person who:* *i. Taking advantage of his influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed taking advantage of his influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favour or on whose account a transaction or act, action, operation or step is made.* *ii. Ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means. Direct ownership is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company. Indirect ownership is a manner of exercising control whereby a company which is under the control of a*

	natural person holds or multiple companies which are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company. *iii. Holds the position of a senior managing official, if, after all possible means of identification have been exhausted, the person specified in clause ii cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner.* *iv. In the case of a trust, civil law partnership, community or legal arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such associations': settlor or person who has handed over property to the asset pool, trustee or manager or possessor of the property, person ensuring and controlling the preservation of property, where such person has been appointed, or the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.*	
	Does the company have Beneficial Owners: YES NO, if No, please explain:	
	Name	Personal ID code/ DOB
	Place of residence	Citizenship
		Shareholding (%)
	Name	Personal ID code/ DOB
	Place of residence	Citizenship
		Shareholding (%)
	Name	Personal ID code/ DOB
	Place of residence	Citizenship
		Shareholding (%)

Members of the MB (in case of legal person)	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till

Authorised persons (representatives)	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
		Power of attorney appended	Valid till

_____

		YES	
	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
		Power of attorney appended YES	Valid till
	Name	Personal ID code/ DOB	
	Place of residence	Copy of the ID document appended YES	Valid till
		Power of attorney appended YES	Valid till

Purpose of the Business Relationship	Please specify

Identification of Politically Exposed Persons (to be filled if relevant)	Record on the Beneficial Owners, members of the MB or authorised representative a Politically Exposed Person. *A Politically Exposed Person is a natural person who is or who has been entrusted with prominent public functions including a head of state, head of government, minister and deputy or assistant minister; 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; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a state-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials.* *• The provisions set out above also include positions in the European Union and in other international organizations.* *• A family member of a person performing prominent public functions is the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a parent of a politically exposed person.* *• A close associate of a person performing prominent public functions is 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; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.* YES NO If Yes, please record the person's name, position (occupation) and links with the politically exposed person.		
	Name	Position (occupation)	Link

	Name	Position (occupation)	Link

Exhibit 1

Exhibit 1a. Contracting states of the European Economic Area

Please refer to http://elik.nlib.ee/pohifakte-euroopa-liidust/liikmesriigid-euroopa-majanduspiirkonna-riigid/

Exhibit 1b. Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies (Text with EEA relevance)

Please refer to https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.254.01.0001.01.ENG

Exhibit 1c. List of risk countries (countries which according to FATF does not follow requirements of prevention of Money Laundering and Terrorism Financing)

Please refer to: http://www.fatf-gafi.org/countries/#high-risk

Exhibit 1c. List of risk countries (countries which according to the FIU are under big threat of terrorism)

Afghanistan, Algeria, United Arab Emirates, Bahrein, Bangladesh, Egypt, Indonesia, Iraq, Iran, Yemen, Jordanian, Qatar, Kuwait, Lebanon, Libya, Malaysia, Mali, Morocco, Mauritania, Nigeria, Oman, Pakistan, Palestine, Saudi Arabia, Somalia, Sri Lanka, Sudan, Syria, Tunisia, Turkey, Ethnic groups of Caucasus belonging to Russian Federation (chechens,lesgid, ossetians, ingushes etc.)

Exhibit 1d. List of countries that are NOT regarded as low tax rate countries

https://www.emta.ee/et/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-eesti-tulu-maksustamine/nimekiri-territooriumidest

_____