APPROVED BY OÜ NeuronEX Platform
Member of the Board Konstantins Grjazevs

18.05.2020

GUIDELINES ON ORGANISATIONAL SOLUTIONS AND PREVENTIVE MEASURES TO TAKE AGAINST MONEY LAUNDERING AND TERRORIST FINANCING (AML/CTF Guidelines)

Version 1.1
Date: 18.05.2020

1. INTRODUCTION

The purpose of these Guidelines on Organizational solutions and preventive measures to take against money laundering and terrorist financing, hereinafter referred to as the "Guidelines", is to set forth the internal practice, measures, procedures and controls of OÜ NeuronEX Platform with regard to the prevention of money laundering and terrorist financing as required by applicable law.

The Guidelines are prepared in order to comply with the provisions of the Money Laundering and Terrorist Financing Prevention Act[1], hereinafter referred as the MLTFPA, International Sanctions Act[2], hereinafter referred as the Sanctions Act and the Financial Intelligence Unit's advisory guidelines[3] (Annex 1), as amended from time to time.

These Guidelines are drafted and shall be periodically reviewed and updated by the AntiMoney Laundering Compliance Officer of the Company, based on the general policy principles laid down by the Board of Directors of the Company with regard to the prevention of money laundering and terrorist financing.

Any amendment and / or modification of these Guidelines shall be drafted in writing and approved by the Board of Directors of the Company in accordance with the provisions of the Articles of Association of the Company.

The Guidelines shall be communicated by the Contact Person to all the employees of the Company who manage, monitor and / or control in any way the transactions of the Clients of the Company and have the responsibility to apply the practices, measures, procedures and controls that have been determined in this Manual and adopted by the Company.

2. DEFINITIONS

2.1.**Money laundering** is property derived from or obtained through criminal activity: the concealment

1 https://www.riigiteataia.ee/en/eli/517112017003/consolide
2 https://www.riigiteataia.ee/en/eli/ee/503072014002/consolide
3 https://www2.politsei.ee/en/organisatsioon/rahapesuandmeburoo/fiusadvisoryguidelines/

or disguise of the true nature, origin, location, manner of disposal, transfer, ownership or other related rights of the property; conversion, transfer, acquisition, possession or use with a view to conceal or disguise the unlawful source of the property or to assist a person who participated in a criminal activity so that he can refrain from the legal consequences of his actions. Money laundering is also covers criminal activity that resulted in money laundering assets occurred in another country.

2.2. **Terrorist financing** is the allocation or collection of funds for the purpose of designing or committing terrorist acts within the meaning of the Penal Code or for financing terrorist organizations, or knowing that these funds will be used for the aforementioned purpose.

2.3. **International Financial Sanctions** are international sanctions which completely or partially prohibit the use and disposal or possession of funds and economic resources in the entity subject of international financial sanctions.

2.4. **The subject of an international sanction** is a natural or legal person, institution, partnership or any other entity directly identified as an instrument imposing or enforcing an international sanction and subject to the measures provided for by an instrument imposing an international sanction.

2.5. **Money Laundering and Terrorist Financing Prevention Act (MLTFPA)** regulates the activities of credit and financial institutions and other companies and institutions provided for in the Money Laundering and Terrorist Financing Prevention Act, as well as the activities of the FIU in combating money laundering and terrorist financing.

2.6. **The Anti Money Laundering Compliance Officer (the Contact Person)** is an employee appointed by the decision of the Board, who is the contact person of the FIU and who ensures the implementation of measures for the prevention of money laundering and terrorist financing in the company.

2.7. **The Responsible Person** is a person appointed by the decision of the Board, who is the responsible person for the FIU and who ensures that by the authority appointed to him the requirements of the INTERNATIONAL SANCTION ACT (RSS) are complied with. The Contact Person can be appointed as the Responsible Person and to be responsible for performing both roles.

2.8. **A client** is a person who uses or has used one or more services offered by the company.

2.9. **Business relationship** within the meaning of this Code of Conduct is the business services provided by the contract with the consumer.

2.10. **A regular client** is a client with whom a contract has been concluded.

2.11. **The FIU** is an independent structural unit of the Police and Border Guard Board whose main task is to prevent money laundering and terrorist financing in Estonia. The FIU analyzes and controls the information received from liable subjects and other parties about suspicion of money laundering or terrorist financing, takes necessary measures to preserve the property, and, if necessary, promptly sends the material to the competent authorities when criminal activity is detected. The main tasks of the FIU are stated in the Money Laundering and Terrorist Financing Prevention Act.
Postal address: Toostuse 52, 10416 Tallinn; email: **rahapesu@politsei**,
online notification form: https://FIUteade.politsei .ee/et/teenused/FIUi
s/.

3. RISK BASED APPROACH

3.1. The Company shall apply appropriate measures and procedures, by adopting a riskbased approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be comparatively higher.

3.2. The Contact Person prepares and regularly at least annually updates and the Board of the Company approves a risk assessment for identifying, assessing and analyzing the risks associated with money laundering and terrorist financing.

3.3. The Contact Person identifies, assesses and analyses at least the following risks:

i. customer risk;
ii. product, service or transaction risk, incl. new and/or future product, service or transaction risk;
iii. risk related to the communication or mediation channels between the obliged entity and customers or to delivery channels and sales of products, services or transactions, incl. such new and/or future channels;
iv. risk related to countries or geographic regions or jurisdictions.

3.4. On the basis of the risk assessment document (Annex 2), the Contact Person determines Company's clients risk scoring model and also determines the situations and conditions whereby Contact Person and/or Compliance department Compliance specialists (hereinafter Compliance specialist(s)) may apply standard or enhanced due diligence measures.

3.5. Upon the assessment of the specific risks related to the Client and the separate business relationship or a person participating in an occasional transaction, the Compliance specialist identifies the risk profile of the Client or the person participating in the transaction and determines the risk level in confluence with the risk profile associated with the business relationship and the risk level (hereinafter jointly the risk profile and risk level).

3.6. Determination of the risk level means that the Compliance specialist considers the activities or actions not expected from certain clients or business relationships to be possible, which is why more attention must constantly be paid to the Client and their activities. Or vice versa, the Compliance specialist does not consider such activities possible from certain clients, which is why the extent of giving attention is different. Determining a risk level that is higher than usual does not mean that the Client launders money or finances terrorism but that more attention must be given to the Client's activities and the circumstances associated with them when considering the circumstances as a set. Neither does determining a lower risk level mean that the Client cannot be associated with money laundering or terrorist financing.

3.7. In order to determine the risk profile and risk level, Compliance specialists take into account:
3.7.1. the risk assessment prepared by the Contact Person;
3.7.2. the purpose of the business relationship or the occasional transaction and the information that the Company has collected about the objective of the business relationship or the occasional transaction ;
3.7.3. the volume of the assets deposited by the Client or the value of an occasional transaction;
3.7.4. the expected duration of the business relationship;
3.7.5. primarily the provisions of Articles 34 and 35 of the MLTFPA as circumstances characterising

lower risk and the provisions of Articles 37, 39, 40 and 41 of the MLTFPA as circumstances characterising higher risk;
3.7.6. the relevant guidelines and instructions of European Union organisations, the Committee of Experts on the Evaluation of AntiMoney Laundering Measures and the Financing of Terrorism of the Council of Europe Moneyval, FATF and the European Supervisory Authorities.

3.8. In accordance with client risk scoring document (Annex 3) there are the following Client risk profile levels:

i. Low risk
ii. Medium risk
iii. Medium Higher risk
iv. High risk.

3.9. A higher risk level must always be determined and enhanced and other relevant due diligence measures must be applied, among others, if:

3.9.1. the customer or the beneficial owner is a politically exposed person;
3.9.2. the Company establishes a correspondent relationship with a highrisk or third country respondent institution;
3.9.3. the Company deals with or provides services to natural persons or legal entities that originate from a highrisk third country or a higher risk country or territory or they have the citizenship of such a country or their place of residence or location or the location of the payee’s payment service provider is in such a country or territory;
3.9.4. transactions are related to complicated, highvalue and unusual transactions and transaction patterns without any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question;
3.9.5. circumstances referring to the risks highlighted Financial Intelligence Unit's advisory guidelines .

3.10. For clients with low, medium and mediumhigher risk profile level standard due diligence procedure is applied. Client file of the client with low risk profile level is reviewed and updated every 12 months. Client file of the client with medium risk profile level is reviewed and updated every 10 months. Client file of the client with mediumhigher risk profile level is reviewed and updated every 8 months.

3.11. For clients with high risk profile level enhanced due diligence procedure is applied. Client file of the client with high risk profile level is reviewed and updated every 6 months.

3.12. The reduction of the risk level from higher to lower level is possible, but this is only done in the case of justified circumstances and considering, among others, the circumstance why giving additional attention to the Client or their activities is no longer necessary. When the risk level is changed in such a manner, the Compliance specialist must be prepared to explain the Contact Person, if necessary, why the risks identified earlier are no longer relevant and why reducing the risk level is justified. The fact that the Client has not concluded transactions referring to the risk that is higher than usual over a certain period of time or has not concluded transactions that the Compliance specialist considered possible upon the determination of a higher risk level does not mean that the Client will not conclude such transactions or perform such actions in the future or that the features and circumstances referring to a higher risk level have been overcome/disappeared.

3.13. Compliance specialist must document the determination of the risk level (i.e. in a client's database), update it and make these data and reasons accessibleto competent authorities as necessary.

4. CLIENT DUE DILIGENCE

4.1. One of the main obligations of the Company in the prevention of money laundering and terrorist financing is the application of preventive measures, i.e. due diligence measures. The primary purpose of application of due diligence measures is to prevent the placement, layering and integration, etc. of criminal proceeds in the various stages of money laundering, prevent the financing of terrorism from illegal or legal sources of money.

4.2. The Company Compliance department Compliance specialists apply due diligence measures:
1) upon establishment of a business relationship;
2) upon making or mediating occasional transactions outside a business relationship where a cash payment of over 15 000 euros or an equal amount in another currency is made, regardless of whether the financial obligation is performed in the transaction in a lump sum or in several related payments over a period of up to one year, unless otherwise provided by law;
3) upon verification of information gathered while applying due diligence measures or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered earlier while updating the relevant data;
4) upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits.

4.3. The application of due diligence measures divides into due diligence upon the establishment of a business relationship and the ongoing monitoring of a business relationship.

4.4. Upon the establishment of the business relationship the following standard due diligence measures are taken by Compliance specialists:
4.4.1. identification of the client and verification of the submitted information by the client based on information obtained from a reliable and independent source.
4.4.2. identification of the person's right of the client representation.
4.4.3. identification of the beneficial owner and, for the purpose of verifying their identity, taking measures to the extent that allows the Company to make certain that the Company knows who the beneficial owner is, and understand the ownership and control structure of theclient.
4.4.4. gathering information on whether a person is a politically exposed person, their family member or a person known to be close associate.
4.4.5. identification of the source and/or origin of wealth if appropriate.
4.4.6. understanding of business relationships or an occasional transaction and, where relevant, gathering additional information thereon.

4.5. The initial data collected in the course of application of due diligence measures is reflected in the client form about the client and provided to the Company by the latter. The client form must include the client's confirmation that the client is aware of and has understood the obligations established with the relevant conditions, incl. the requirement to submit the information necessary for the establishment of the business relationship and the format of such information as well as the responsibility associated with such data not being true.

4.6. Upon the monitoring of the business relationship the following standard due diligence measures are taken by Compliance specialists:
4.6.1. checking of transactions made during business relationship in order ensure that the transactions

correspond to the Company's knowledge of the customer, their activities and risk profile.
4.6.2. regular updating of relevant documents, data or information gathered in the course of application of due diligence measures.
4.6.3. identification of the source and origin of the funds used in a transaction.

4.7. Proceeding from the above, the primary requirement of the measures of money laundering and terrorist financing prevention is that the Company does not enter into transactions or establish relationships with anonymous or unidentified persons. The Company refuses to conclude a transaction or establish a business relationship if the Client does not submit as much information as required for their identification or about the objectives of transactions or if their activities create suspicions of money laundering or terrorist financing. In certain cases as stipulated in this Guidance, the Company is obliged to exercise it's right and refuse the transactions concluded within the scope of the business relationship. The Company is obliged to terminate a longterm contract without notice if the person does not submit sufficient information for the application of due diligence measures.

5. CLIENT IDENTIFICATION

5.1. Identification of a natural person.

5.1.1. Upon establishment of the business relationship or the completion of an occasional transaction, the Compliance specialist must identify the natural person, who is the Client or the person participating in an occasional and verify the submitted information on the basis of the information obtained from a reliable and independent source.

5.1.2. Compliance specialist must ascertain whether the person is acting on behalf of themselves or another person (natural person or legal entity). If the person acts on behalf of another person, Compliance specialist also identify that another person, i.e., beneficial owner.

5.1.3. Knowing the Client personally or the fact that they are publicly known is not a basis for non implementation of the internal procedure for identification stipulated by law. Persons who are publicly known and persons directly or indirectly related to them who contact the Company in order to conclude a transaction or perform an act must also be identified.

5.1.4. Identity must always be ascertained and verified within reasonable time before the initiation of the actions related to the entry into a longterm contract or at the time of entry into such a contract. A person who participates in a transaction must be identified before the commencement of the acts of completing the transaction or during the completion of the transaction.

5.1.5. Identification means ascertaining the identity of a person on the basis of the personal and personalised unique information directly related to the person. The following data (or hereinafter information within the meaning of these Guidelines) are used, collected and retained for identification:

i. the person's name;
ii. the person's personal identification code, or if the person doesn't have one, their date and place of birth and place of residence or location,
as well as other data directly related to the person, such as:
iii. place of residence;
iv. profession or area of activity, if necessary

5.1.6. The following documents are used for identification:

i. a document specified in subsection 2 (2) of the Identity Documents Act[4];
ii. a valid travel document issued in a foreign country;
iii. a driving licence that complies with the conditions stipulated in subsection 4 (1) of the Identity Documents Act; or
v. a copy of the aforementioned documents that has been authenticated by a notary, certified by a notary or officially certified.

5.1.7. Upon the demand of the Company, the Client submits the documents and provides the information required for identification. Upon the demand of the Company, the Client confirms with their signature that the information and documents submitted for the application of the due diligence measures are true.

5.1.8. Verification of the information obtained in the course of identification means using data from a reliable and independent source to confirm that the data are true and correct, also confirming, if necessary, that the data directly related to the person are true and correct. This means that the purpose of verification of information is to obtain reassurance that the person who wants to establish a business relationship or conclude an occasional transaction is the person they claim tobe.

5.1.9. Verification of information collected in the course of identification of a person must be carried out facetoface or with an IT device (i.e., video or online identification).

5.1.10. Facetoface identification means that the Client or their representative and the representative of the Company are in the same place within the scope of a specific meeting. This means that the potential Client or their representative has direct contact with the representatives of the Company in the course of which the representative of the Company compares the person's biometrics (facial image) with the facial image on or obtained from the identification document. Direct contact requires direct communication between the representative of the Company and the Client or their representative to assess the compliance of the content of their declaration of intent and goal with the actual intent. The contact may take place outside the permanent place of business of the Company if at least the same due diligence obligations that are performed in ordinary cases are performed in its course.

5.1.11. In the case of identification with an IT device, the Company complies with the requirements stipulated in § 31 of the MLTFPA and the technical requirements and procedure specified in the regulation of the Minister of Finance established on the basis of the authorisation provision stipulated in subsection (6) of the same section. The objective, among others, is to compare the person's biometrics (facial image) obtained in the course of thesession

4 https://www.riigiteataia.ee/en/eli/ee/513042015004/consolide/current

with the facial image on or obtained from the identification document.

5.1.12. The (i) facetoface identification or (ii) identification with an IT device or (iii) identification on the basis of the copy of an identity document authenticated by a notary or certified by a notary or officially certified and when seeing the original of the copy in respect of the Client and/or representative of the Client is deemed to be the reliable and independent verification of the information obtained in the course of identification because an identity document that is valid and issued by an independent state authority is seen during this.

5.1.13. Irrespective of the selected reliable and independent source, the Compliance specialist must make sure in the case of identity documents that (i) the document is valid and complies with the requirements stipulated in the Identity Documents Act and (ii) the person resembles the person depicted on the document photo in terms of appearance and age and the data included in the document.

5.1.14. In the case of representation, the Compliance specialist must also identify and verify the nature and scope of the right of representation. If the right of representation does not arise from law, the name, date of issue and name of issuer of the document that serves as a basis for the right of representation must be ascertained and retained.

5.1.15. The representative of a foreign legal entity must submit, on the request of the Compliance specialist, a document that proves their authorisation and has been certified by a notary or in an equivalent manner and that has been legalised or certified with a certificate that replaces legalisation (Apostille), unless otherwise stipulated in the international agreement.

5.1.16. When the right of representation of authorised and legal representatives is handled, it must be ascertained by the Compliance specialist whether the representative knows their customer. In order to ascertain the nature of the actual relationships between the representative and the represented person, the representative must know the content and objective of the declarations of intent of the person they represent, and they must also be able to answer other relevant questions about the represented person's location, areas of activity, turnover and transaction partners, other related persons and beneficial owners. The representative must also confirm that they are aware of and convinced about the source and legal origin of the funds used by the represented person in the transaction.

5.1.17. Upon the identification of a natural person, the Compliance specialist must also identify the beneficial owner of the natural person, i.e. the person who controls and benefits from the person's activity. Suspicions about the existence of a beneficial owner may arise primarily if, upon the implementation of due diligence measures, the Compliance specialist has noticed that the natural person has been influenced to establish the business relationship or conclude the transaction. In such a case, the person who exercises control over the natural person must be considered the beneficial owner of the natural person.

5.2. Identification of a legal entity.

5.2.1. Upon the establishment of a business relationship or the completion of an occasional transaction, the Compliance specialist must identify the legal entity who is the Client or the legal entity participating in an occasional transaction and verify the submitted information based on information obtained from a reliable and independent source, incl. using means of electronic identification and of trust services for electronic transactions.

5.2.2. The representative of a legal entity is identified and the obtained data are verified on the basis of point 5.1. of these Guidelines.

5.2.3. The Compliance specialist must identify the Client and verify the identification data within reasonable time before the initiation of the actions related to the entry into a longterm contract or at the time of entry into such a contract. A person who participates in a transaction must be identified before the commencement of the acts of completing the transaction or during the completion of the transactions.

5.2.4. Identification means the collection and retention of the following data:

i. business name or name (with the legal form) of the legal entity;
ii. registry code or registration number and date;
iii. name of the director or names of members of the management board or members of another equivalent body, and their authorities in representing the legal entity, whereby the representative who wants to establish a customer relationship is identified and the obtained data are verified according to the requirements of point 5.1. of these Guidelines;

also the collection and retention of other data directly related to the person, such as:

i. location of the legal entity, whereby the theory of the country of establishment must be proceeded from;
ii. place of business of the legal entity;
iii. data of the means of communication of the legal entity.

5.2.5. The following documents are used for identification:

i. registry card of the relevant register;
ii. registration certificate of the relevant register; or
iii. a document equivalent with an aforementioned document or relevant document of establishment of the legal entity.

5.2.6. Upon the demand of the Compliance specialist, the Client submits the documents and provides the information required for identification. Upon the demand of the Compliance specialist, the Client confirms with their signature that the information and documents submitted for the application of the due diligence measures are true. If the Company has access to the relevant registers, Compliance specialists do not have to ask the Client to provide the relevant documents used foridentification.

5.2.7. Verification of the information obtained in the course of identification means using data from a reliable and independent source to confirm that the data collected during identification process are true and correct, also confirming that the data directly related to the person are true and correct. This means that the purpose of verification of information is to obtain reassurance that the person who wants to establish a business relationship or conclude an occasional transaction is the person they claim to be.

5.2.8. A source is deemed to be reliable and independent if the Compliancespecialist:

i. sees the original of the document specified in point 5.2.5. of these Guidelines;
ii. sees a copy of the document specified in point 5.2.5. of these Guidelines that has been authenticated by a notary, certified by a notary or officially certified;
iii. has access to the data in the Commercial Register, Register of Nonprofit Associations and Foundations or the relevant registers of foreign countries via a computer network.

5.2.9. The documents issued by the registers may not have been issued earlier than six months before

their submission to the Company. This also applies if a copy has been made of the document.

5.2.10. In situations not specified in point 5.2.8. of these Guidelines, the reliable and independent source is the verification of the information obtained in the course of identification, which originates from two separate sources.

5.2.11. Within the meaning of point 5.2.10. of these Guidelines, two different sources means that the data medium, place or measure of obtaining information must be different (i.e. it cannot be the same data medium).

5.2.12. In addition to the document specified in point 5.2.5. of these Guidelines (if the Compliance specialist does not select two different identity documents of the Client for verification), the second source may also be information obtained from a reliable and independent source for checking the data directly related to the person (such as the location, etc.).

5.2.13. Public documents issued in a foreign country must be legalised or confirmed with a certificate (an Apostille), i.e. an internationally recognised official certification of the authenticity of the document has been issued for use of an official document issued in one country in another country, whilst legalisation and the attachment of an Apostille does not confirm that the information in the document is true.

5.2.14. A document must be legalised if it is not subject to confirmation with an Apostille. For legalisation, a document must pass the legalisation authorities of the issuing country and the receiving country of the document (usually ministries of foreign affairs).

5.2.15. At the same time:

i. public documents prepared or certified in countries with whom Estonia has entered into the relevant legal assistance agreement do not require legalisation or an Apostille;
ii. legalisation or an Apostille is not required for public documents issued in a country that implements the Convention Abolishing the Legalisation of Documents in the Member States of the European Communities.

5.2.15. In the case of documents in foreign languages, the Compliance specialist has the right to demand translation of the documents to a language they understand (e.g., English). The use of translations should be avoided in situations where the original documents are prepared in a language understandable to the Compliance specialist (e.g. in English).

5.2.16. Upon the establishment of a business relationship or the completing an occasional transaction, the Compliance specialist must identify the beneficial owner of the Client or the person participating in the occasional transaction and take measures to verify the identity of the beneficial owner to the extent that allows the Compliance specialists to make sure that they know who the beneficial owner is.

5.2.17. The beneficial owner means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or exercises control in another manner over a transaction, act , action, operation or step or over another person and/or in whose interests or for whose benefit or on whose account a transaction or act, action, operation or step is made.

5.2.18. The Compliance specialist must understand the ownership and control structure of the Client or the person participating in an occasional transaction upon the establishment of a business

relationship or the completion of an occasional transaction.

5.2.19. The beneficial owner of a legal entity is identified in stages where the Compliance specialist proceeds to each subsequent stage if the beneficial owner of the legal entity cannot be determined in the case of the previous stage. The stages and questions are as follows:

i. is it possible to identify, in respect of the Client that is a legal entity or a person participating in the transaction, the natural person or persons who actually ultimately control the legal entity or exercise influence or control over it in any other manner, irrespective of the size of the shares, voting rights or ownership rights or its direct or indirect nature;
ii. whether the Client that is a legal entity or the person participating in the transaction has a natural person or person who owns or controls the legal entity via direct or indirect shareholding. Family connections and contractual connections must also be taken into account;
iii. who is the natural person in senior management, who must be defined as the beneficial owner, as the answers to the previous two questions have not made it possible for the Compliance specialist to identify the beneficial owner.

5.2.20. A member of senior management specified in point 5.2.19. of these Guidelines is a person who:

i. makes the strategic decisions that fundamentally affect business activities and/or practices and/or the company general (business) trends; or in its absence
ii. carries out everyday or regular management functions of the company within the scope of executive power (e.g. chief executive officer (CEO), chief financial officer (CFO), director or president , etc.).

5.2.21. The Compliance specialist takes measures to verify the identified beneficial owner and does the same to an extent that makes it possible for the Compliance specialist to conclude that they know who the beneficial owner is.

5.2.22. In the case of legal entities, this requires, (i) in the case of identifying the purpose and nature of the business relationship, making it possible for Compliance specialist to conclude that the Client's beneficial owner, if the latter participates actively in the company's activities, is capable of operating in the declared area of activity, with the declared scope of activity and with the declared main business partners and has the required experience; and (ii) that the Compliance specialist:

i. sees the original of the document specified in point 5.2.5. of these Guidelines;
ii. has access to the data in the Commercial Register, Register of Nonprofit Associations and Foundations or the relevant registers of foreign countries via a computer network and checks the beneficial owner's data in said register;
iii. sees a copy of the document specified in point 5.2.5. of these Guidelines that has been certified by a notary or officially certified;
iv. uses other publicly accessible and/or reliable sources that are sufficient to make it possible to conclude who the beneficial owner is.

5.2.23. If the identity documents of the legal entity or the other submitted documents do not indicate directly who the beneficial owner of the legal entity is, the relevant data (incl. data about being a member of a group and the ownership and management structure of the group) are registered by the Compliance specialist on the basis of the statement of the representative of the legal entity or the document written by hand by the representative of the legal entity. In such a case, the Compliance

specialist must take reasonable measures to verify the submitted information.

5.2.24. The Compliance specialist must not independently inspect the ownership and control structure of a Client or a person concluding an occasional transaction and may rely on the statements or written explanations of the representative of the legal entity. This does not apply if the Compliance specialist has information that casts doubt on said circumstance, incl. it is in contravention of the data obtained in the course of identification of the beneficial owner and the verification of data.

5.3. Identification of a politically exposed person.

5.3.1. Both upon the establishment of a business relationship as well as in the course of a business relationship or if a certain trigger event occurs, the Compliance specialist will take measures to ascertain whether the Client or the person who wants to conclude an occasional transaction and the beneficial owner or representative of these persons is a politically exposed person, their family member or close associate, or if the customer has become such a person.

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

5.3.3. Politically exposed person means at least a natural person who is or who has been entrusted with prominent public functions, incl. 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 charge d'affaires and a high ranking officer in the armed forces; a member of an administrative, management or supervisory body of a Stateowned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middleranking or more junior officials.

5.3.4. In the case of a Client that is a legal entity or a person concluding an occasional transaction, the person must be considered a politically exposed person if their representative or beneficial owner is a politically exposed person or a family member or close associate of the politically exposed person.

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

5.3.6. A person known to be close associate is:

i. a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal entity or a legal arrangement, or any other close business relations, with a politically exposed person;
ii. 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 exposedperson;
iii. who is known to have a relationship with the beneficial owner that does not quality as the status of a family member (e.g. boyfriend or girlfriend, mistress, etc.).

5.3.7. A politically exposed person can be identified by the Compliance specialist in the following

ways:

i. screening of new, potential and existing clients or persons who want to conclude occasional transactions, their beneficial owners and representatives against the relevant internal or external databases (i.e. name checks in databases) that provide the relevant service;
ii. asking the representative (covers asking the representative and beneficial owner as well as their family members and close associates) or the person concluding an occasional transaction about the status of a politically exposed person, also asking, where necessary, the Client or the person concluding an occasional transaction about their profession or area of activity and asking the aforementioned data again during the updating of data carried out in the course of the business relationship;
iii. in certain cases, obtaining information about the person from public accessible or third sources in addition to the information specified in the previous point.

5.3.8. In addition to the standard due diligence measures specified in these Guidelines, the Compliance specialist applies the following due diligence measures to politically exposed person:

i. obtains the approval from the senior management, i.e., Contact Person and board member of the Company, to establish or continue a business relationship with the person;
ii. applies measures to establish the source and/or origin of the wealth of the person and the sources of the funds that are used in the business relationship or upon executing occasional transactions;
iii. monitors the business relationship in an enhanced manner.

5.3.9. Establishment of the source and/or origin of wealth means that the Compliance specialist identifies a bigger and more general picture of the Client's wealth, i.e. the source of all assets. This usually indicates how many funds the Client may have at all and where the Client received these funds from. In addition to requesting the relevant information from the Client, it may also be possible to collect such information from public databases and other public or nonpublic data, such as the land register, registers of other assets, declarations of economic interests, registers of companies, etc. However, the data of the source and/or origin of wealth must be verified on the basis of reliable and independent data, documents and information if the risk associated with the Client is particularly high. The Compliance specialist should not settle for the general answers of the Client or make unjustified assumptions (e.g. that employees with significant functions have bigger salaries and more assets etc.) and the Compliance specialist must be convinced that they know the source and/or origin of the Client's wealth. If the customer refuses to disclose data about the source and/or origin of their wealth or gives general answers or the data differ from the data that are publicly or nonpublicly accessible, this may be a situation that points at a higher risk to which enhanced attention must be given, i.e. with regard to which enhanced measures must be taken.

6. IDENTIFICATION OF THE SOURCE AND/OR ORIGIN OF WEALTH.

6.1. The Compliance specialist collects information about the source and/or origin of the customer's wealth (i) upon the establishment of a business relationship, if appropriate, to identify the purpose and nature of the business relationship, also if (ii) the Compliance specialist suspects that the customer or the person concluding an occasional transaction is a politically exposed person, their family member or close associate.

6.2. In the case of an occasional transaction outside a business relationship, the Compliance specialist collects information about the source and/or origin of the wealth instead of the purpose and nature of the business relationship in the appropriate case. The Compliance specialist also takes other measures if necessary, which are stipulated under the identification of the purpose and nature of a business

relationship within the meaning of these Guidelines.

6.3. Within the meaning of these Guidelines, identification of the source and/or origin of wealth means the measures described in point 5.3.9. of these Guidelines.

7. IDENTIFICATION OF THE PURPOSE AND NATURE OF A BUSINESS RELATIONSHIP OR OCCASIONAL TRANSACTION.

7.1. In the case of the establishment of a business relationship or an occasional transaction, the Compliance specialist must understand the purpose and nature of the business relationship or transaction. This is one but a significant, part of the implementation of the KnowYourClient principle.

7.2. In the appropriate case, the Compliance specialist must take additional measures and collect additional information to identify the purpose and nature. Such an appropriate situation occurs primarily in the cases where (i) there is a situation that refers to high value or is unusual and/or (ii) where the risk and/or risk profile associated with the Client and the nature of the business relationship gives reason for the performance of additional actions in order to be able to appropriately monitor to business relationship later.

7.3. The additional measure specified in point 7.2. of these Guidelines means, among others, making queries in public sources and additional information is ascertaining the permanent area of activity, payment practices, main transaction partners and, in the case of a legal entity, the experience of the Client or the person participating in an occasional transaction. The above is not an exhaustive list and, if necessary, the Compliance specialist takes additional measures to understand the purpose and nature of the business relationship, incl. primarily identifies the source and/or origin of wealth, where necessary, and performs onsite visits before the establishment of the business relationship, etc.

7.4. Identification of the purpose and nature of the business relationship and occasional transaction is the most important principle of the due diligence measures. The objective is to obtain a comprehensive understanding and overview of the Client, incl. the person, the beneficial owners and the Client profile as well as the reasons why a specific service is needed. The Compliance specialist thereby makes sure that the service provided complies with the content of the Client's actual declarations of intent (why they want the financial service), complies with the nature and purposes of the specific contract and corresponds to the risk level assigned to the Client. The Compliance specialist must assess on the basis of the aforementioned information what the expected activities of the Client are like, i.e. on the basis of this information it will be possible for the Compliance specialist to later assess the activities of the Client against the information already collected (to constantly observe/monitor the transactions concluded within the business relationship, incl. to identify the source and origin of the funds used in the transaction). On the basis of this information, it is also possible to assess whether the person, their representative or beneficial owner could be a politically exposed person, whether the beneficial owner is the real beneficial owner, i.e. whether they have the capacity to conclude transactions of such volume and with the main business partners and whether there is a chance that the Client, their representative or beneficial owner is actually a person under international sanctions or that the transactions of the customer are attempts to avoid an international sanction.

7.5. If the objective on one hand is to obtain a comprehensive understanding and overview of the Client (point 7.4. of these Guidelines), the objective is also to understand and ensure that such a wish of the Client complies with their actual activities, capability, capacity and needs.

7.6. As is the case with all other due diligence measures, the riskbased approach must be proceeded from when the purpose and nature of the business relationship are identified. The bigger the risk

associated with the Client, the more measures the Compliance specialist must take to understand the Client and their risk profile and to understand whether the KnowYour Client principle has been followed and whether it is unambiguously understandable which service the Client wants to get and why, i.e. whether this wish corresponds to their actual activities, capacity and needs. Information may not be vague in such cases.

7.7. In order to identify the area of activity, the obliged entity must understand what the Client deals with and intends to deal with in the course of the business relationship and how this corresponds to the purpose and nature of the business relationship in general and whether it is reasonable, understandable and plausible. The identification of the area of activity does not mean noting down the data entered in registers, but an actual understanding of what the Client is doing and the retention of the relevant data.

7.8. The aforementioned area of activity must thereby fit into the experience profile of the Client's representative (or key persons) and/or the beneficial owner. The performance of this obligation often, and especially in the case of a suspicion, calls for the more general identification of the source and/or origin of the Client's wealth.

8. CLIENT DUE DILIGENCE DURING THE BUSINESS RELATIONSHIP / ONGOING MONITORING.

8.1. Updating data.

8.1.1. The Compliance specialist ensures that the documents, data or information collected in the course of the application of due diligence measures are updated regularly and in the case of trigger events, i.e. primarily the data concerning the person, their representative (incl. the right of representation) and beneficial owner as well as the purpose and nature of the business relationship.

8.1.2. In the case of clients and business relationships whose risk is high, the existing data must be verified more frequently than in the case of other customers / business relationships. The data of the clients and business relationships must usually be updated at least once a year.

8.2. Ongoing monitoring of business relationship.

8.2.1. During the business relationship, the Compliance specialist monitors the business relationship, which covers transactions carried out in the business relationship to ensure that the transactions correspond to the Company's knowledge of the Client, their activities and risk profile. Monitoring of the business relationship covers the entire business relationship and its life cycle, incl. incoming transactions to which a separate requirement for identification of the source and origin of the funds used in the transaction is applied.

8.2.2. In the course of the ongoing monitoring of a business relationship, the Compliance specialist must monitor the transactions concluded during the business relationship in such a manner that the Compliance specialist can determine whether the transactions to be concluded correspond to the information previously known about the Client (i.e. what the Client declared upon the establishment of the business relationship or what has become known in the course of the business relationship). The Compliance specialist must also monitor the business relationship to ascertain the Client's activities or facts that indicate criminal activities, money laundering or terrorist financing or the relation of which to money laundering or terrorist financing is probable, incl. complicated, highvalue and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or that are uncharacteristic of the specific features of the business in question.

8.2.3. In the course of the business relationship, the Compliance specialist must also constantly assess the changes in the Client's activities and assess whether these changes may increase the risk level associated with the Client and the business relationship, giving rise to the need to apply additional or enhanced due diligence measures, incl. in the situation where the person is actually a politically exposed person, the beneficial owner is someone else or the aim of the customer's activity is to avoid an international sanction.

8.2.4. In such a manner, the Compliance specialist constantly assesses whether the purpose and nature of each single transaction correspond to what was already ascertained in the course of the application of due diligence measures upon the establishment of the business relationship,
i. e. the information previously known about the Client. The Compliance specialist must thereby select the suitable scope of implementation of due diligence and, based on this, collect sufficient data and documents. The objective is to obtain an adequate overview of the Client or the person taking part in the transaction, incl. an overview of the Client and the Client's profile, and the reasons why the specific transaction is concluded and within the scope of which economic or legal relationships the customer concludes transactions, in order to assess, if necessary, whether it corresponds to the information already known.

8.2.5. As is the case with all other due diligence measures, the riskbased approach stipulated in these Guidelines must be followed here as well. The higher the risk/threat associated with the Client, the more the Compliance specialist must take measures to understand the Client and
their risk profile and the single transaction carried out within the scope of the business relationship and be sure that it corresponds to the information previously known about the Clients. Information may not be vague in such cases.

8.2.6. The Compliance specialist acknowledges and takes measures to identify in the course of monitoring of the business relationship, among others, whether the Client in the business relationship is the person that they claimed to be, or whether the person is a politically exposed person or other beneficial owner or whether they want to avoid international sanctions within the scope of the business relationship.

8.2.7. Transaction monitoring measures, which are used by the Compliance specialist, are divided into two categories: measures that are used to monitor (screen) transactions in real time on the basis of the parameters or characteristics developed in internal risk assessment of the Company (Annex 1, 2 and 3) (IT measures) and measures that can be used to analyse (monitor) transactions later.

8.2.8. The monitoring of complicated, highvalue and unusual transactions and transaction patterns that have no reasonable or obvious economic or legitimate purpose or that are uncharacteristic of the specific features of the business in question forms a significant part of the due diligence measures implemented by the Company and makes it possible to identify circumstances in the economic activities of clients that may refer to money laundering and terrorist financing. The monitoring of business relationships for the aforementioned purposes also has a role in the identification of subjects of international sanctions or transactions restricted with sanctions and politically exposed persons.

8.2.9. According to the monitoring of transactions in real time, customer service employees and Compliance specialists monitor the Client's behaviour and transactions upon the performance of their duties in order to identify (i) suspicious and unusual transactions and transaction patterns, (ii) transactions that exceed the established thresholds, or (iii) politically exposed persons and circumstances related to international sanctions.

8.2.10. The Company does the following combination of the following measures to monitor business relationships and transactions in real time as described in these Guidelines:

i. use an IT solution, i.e. automatic IT systems (e.g., Ondato, Coinfirm and/or internally build IT systems) that select real time transactions on the basis of the parameters given; and
ii. assign an employee of the obliged entity the obligation to review transactions manually.

8.2.11. Transactions that have been separated from the mass of transactions later on the basis of certain parameters (mentioned in internal risk assessment document Annex 2) are analysed for monitoring by the Compliance specialists.

8.2.12. According to transaction monitoring, customer service employees and Compliance specialists of the Company observe the client's behaviour and transactions upon the performance of their duties in order to identify transactions and circumstances that could not be identified in real time (they could not be intervened in, such as transactions made via ATMs) or that, due to the nature of the transaction, did not appear in the parameters of monitoring transactions in real time in the case of the IT solution or in acts in the case of manual monitoring (e.g. larger transactions by amounts, currencies or high risk clients).

8.2.13. The Compliance specialist must pay enhanced attention or apply enhanced due diligence measures to transactions and transaction patterns that are complicated, highvalue and unusual and that have no reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

8.2.14. The Compliance specialist registers and retains information about all acts carried out to ongoing monitor the business relationship, i.e. check whether the transactions carried out by the Client correspond to what the obliged entity knew about the customer before.

8.3. <u>identification of the source and origin of funds used in a transaction.</u>

8.3.1. In the course of the business relationship, the Compliance specialist identifies the source and origin of the funds used in a transaction if necessary.

8.3.2. Asking about the source and origin of the funds used in the transaction is basically equivalent to the monitoring of the business relationship within the meaning of these Guidelines and the objective provided therein, with the difference being that whilst the monitoring of the business relationship covers the entire business relationship of the Client and its lifecycle, the source and origin of the funds used in a transaction are only related to incoming transactions. However, the goal is still the same to obtain an adequate overview of the Client and find out whether this corresponds to the information previously known about the Client.

8.3.3. If the monitoring of the business relationship is ongoing, including the entire business relationship of the Client and its life cycle (thereby also covering incoming transactions in general) and this does not depend on the need, the source and origin of the funds used in the transaction must be identified when necessary. The need to identify the source and origin of funds depends on the Client's previous activities as well as other known information.

Thereby the need for identification of the source and origin of the funds increases:

i. proportionally to the size of the funds;
ii. if the transactions do not correspond to the information previously known about the Client;

iii. if the Compliance specialist wants to or should reasonably consider it necessary to assess whether the transactions correspond to the information previously known about theClient;
iv. if the obliged entity suspects that the transactions indicate criminal activities, money laundering or terrorist financing or that the relation of transactions to money laundering or terrorist financing is probable, incl. complicated, highvalue and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

9. ENHANCED DUE DILIGENCE.

9.1. The Compliance specialist must apply enhanced due diligence measures if they have identified that the risk of money laundering or terrorist financing in the case of the Client and their activities is higher than usual. Enhanced due diligence measures are applied in order to appropriately manage and mitigate the risk of money laundering and terrorist financing that is higher than usual.

9.2. An enhanced due diligence measure means that the Compliance specialist applies something in addition to the mandatory main due diligence measures.
9.3. Enhanced due diligence measures can be applied to the Client upon the establishment of a business relationship or to the transaction carried out by the Client during the business relationship or in the case of an occasional transaction.

9.4. The Compliance specialist considers the provisions of the Guidelines on risk based approach when deciding on the application of enhanced due diligence measures to the Client or their transaction, whilst enhanced due diligence measures always mean the reassessment of the Client's risk profile six months after the establishment of the business relationship. Enhanced due diligence measures may, among others, also be

9.4.1. the following upon the establishment of a business relationship:

i. identification of all beneficial owners of the company, incl. those whose shareholding is below 25%;
ii. carrying out an independent assessment of the Client and, if necessary, obtaining the approval of the senior management about new and existing clients on the basis of risksensitivity;
iii. identification of the reasons and circumstances why the Client uses complicated ownership structures and/or has registered the company in the specific country;
iv. obtaining information about the source and/or origin of the wealth of the Client and their beneficial owner.

9.4.2. the following in the course of the ongoing monitoring of the business relationship:

i.monitoring the business relationship more efficiently by increasing the number and frequency of applicable verification measures and selecting the transaction indicators that will be additionally checked;
ii. 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.

9.5. Upon the selection of enhanced due diligence measures, the Compliance specialist considers:

9.5.1. among others, the money laundering and terrorist financing risks and methods specific to the Company business;

9.5.2. that the due diligence measure mitigates the identified higherthanusual risk of money laundering and terrorist financing, is effective and proportionate in respect of this risk and takes it into account.

10. RELYING ON A THIRD PARTY.

10.1. The Compliance specialist relies on a third party in a situation where a third party implements the requirements arising from the MLTFPA for the performance of their obligations arising from law, after which the obliged entity uses them in the performance of their obligations and relies on these data. This obligation differs from outsourcing where a third party implements the requirements arising from the MLTFPA on behalf and for the account of theCompany.

10.2. The Compliance specialist may rely on the data and documents gathered by another person upon the partial or full application of the due diligence measures specified in these Guidelines (i.e. the identification of the customer, beneficial owner and politically exposed person) if the Compliance specialist:

i. gathers from the third party at least information on who is the person establishing the business relationship or making the transaction, their representative and the beneficial owner, as well as what is the purpose and nature of the business relationship or transaction;
ii. has ensured that, where necessary, it is able to immediately obtain all the data and documents whereby it relied on data gathered by another person;
iii. has established that the other person who is relied on is required to comply and actually complies with requirements equal to those established in the relevant directives of the European Parliament and of the Council, including requirements for the application of due diligence measures, identification of politically exposed persons and data retention, and is under or is prepared to be under state supervision regarding compliance with the requirements.

10.3 The Compliance specialist is not allowed to rely on an entity that has been established in a high risk third country.

10.4. The Company, when it relies on the third party, is responsible for compliance with requirements and therefore also for any violations.

11. TRANSACTIONS WITH CLIENTS FROM HIGHRISK THIRD COUNTRIES.

11.1. If the Company has contact with a highrisk third country via a transaction carried out in their economic activities or the Client, the Compliance specialist must apply the following due diligence measures in addition to the ordinary due diligence measures:

11.1.1. gathering additional information about the customer and their beneficial owner;
11.1.2. gathering additional information about the planned substance of the business relationship;
11.1.3. gathering information about the source and/or origin of the funds and wealth of the Client and their beneficial owner;
11.1.4. gathering information about the underlying reasons of planned or executed transactions;
11.1.5. obtaining permission from the senior management to establish or continue a business relationship;
11.1.6. improving the monitoring of a business relationship by increasing the number and frequency of the applied control measures and by choosing transaction indicators that are additionally verified.

12. DATA RETENTION.

12.1. The obliged entity must register and retain:

12.1.1. information about the circumstances of refusal of the establishment of a business relationship or the completing an occasional transaction by the Company;
12.1.2. information if it is impossible to take the due diligence measures using information technology means;
12.1.3. the circumstances of refusal to establish a business relationship or to conclude a transaction, incl. an occasional transaction, on the initiative of a person participating in the transaction or the Client if the refusal is related to the application of due diligence measures by the Company;
12.1.4. originals or copies of the documents that serve as a basis for the establishment of identity and verification of the submitted information. If a person has been identified digitally, i.e. without being in the same place with the person, the data of the document for digital identification, the information about the making of an electronic query in the database of identity documents and the sound and video recording of the identification and verification procedure as well as other data (logs, etc.), which prove the verification of the data obtained in the course of identification (incl. the existence of two separate sources), must be registered and retained according to the selected measure. Data must not be registered and retained to the extent in which the Company is capable of reproducing the aforementioned data during the fiveyear time period for data retention. The Company must be capable of showing at all times that they have verified the data obtained in the course of identification and indicate the reliable and independent source of the data as well as the origin of the twosources;
12.1.5. the documents that serve as a basis for the establishment of the business relationship but not specified in these Guidelines;
12.1.6. the transaction date or period and a description of the substance of the transaction;
12.1.7. data and documents collected in the course of monitoring the business relationship, incl. the documents covering all analyses related to understanding transactions and measures for identifying the background and objective of complicated, highvalue and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or uncharacteristic of the specific features of the business in question);
12.1.8. all of the correspondence related to the performance of the obligations arising from these Guidelines and the MLTFPA;
12.1.9. the information that serves as a basis for the obligation to report to the Financial Intelligence Unit;
12.1.10. data of suspicious or unusual transactions or circumstances of which the Financial Intelligence Unit was not notified.
12.1.11. information about the circumstances of termination of the business because the application of due diligence measures is impossible.

12.2. The data arising these Guidelines must be retained for five years after the expiry of the business relationship or the completion of an occasional transaction. The data related to the performance of the reporting obligation must be retained for five years after the performance of the reporting obligation.

12.3. The Company deletes the retained data after the expiry of the time period, unless the legislation regulating the relevant field establishes a different procedure. On the basis of a precept of the competent supervisory authority, data of importance for prevention, detection or investigation of money laundering or terrorist financing may be retained for a longer period, but not for more than five years after the expiry of the first time period.

12.4. Documents and data must be retained in a manner that allows for exhaustive and immediate

response to the queries made by the Financial Intelligence Unit or, pursuant to legislation, other supervisory authorities, investigation authorities or the court. This also covers data about whether the obliged entity has or has had a business relationship with the person specified in the query within the previous five years and what the nature of this relationship is or was.

13. REFUSAL TO ESTABLISH BUSINESS RELATIONSHIPS OR CARRY OUT OCCASIONAL TRANSACTIONS.

13.1. The Company (i.e., Contact Person and member of the board) refuse to establish a business relationship or allow to execute an occasional transaction if:

13.1.1. they suspect money laundering or terrorist financing or it is impossible for the Company to apply the due diligence measures taken upon the establishment of business relationships, because the Client does not submit the relevant data or refuses to submit them or the submitted data give no grounds for reassurance that the collected data are adequate;
13.1.2. a person whose capital consists of bearer shares or other bearer securities wants to establish a business relationship or conclude an occasional transaction;
13.1.3. a person who does not have the authorisation to operate as a credit or financial institution, but whose main and permanent economic activities via the obliged entity are similar or correspond to the provision of financial services subject to authorisation, wants to establish a business relationship or conclude an occasional transaction;
13.1.4. this would require the opening of an anonymous account, as well as the opening of an account clearly in the name of the wrong person;
13.1.5. a natural person behind whom is another, actually benefiting person, wants to establish business relationship or conclude an occasional transaction (suspicion that a front is used);
13.1.6. the Client, representative and/or beneficial owner is from a country, which is listed as non serviced country by the Company;
13.1.7. the Client, representative and/or beneficial owner is listed on the EU, UN or US sanctions lists ;
13.1.8. the Client, representative and/or beneficial owner is involved in restricted business activities.

13.2. The Company has the right to refuse to make a transaction where a person participating in a transaction or a Client, in spite of a respective request, does not submit documents and relevant information or data or documents proving the origin of the assets constituting the object of the transaction or the purpose of the transaction or where the data and documents submitted make the Company suspect money laundering or terrorist financing or the commission of related crimes or an attempt at such activity.

13.3. If the data are insufficient or untrue or if there are suspicions of money laundering or terrorist financing, the Compliance specialist must apply due diligence measures for as long as they have collected sufficient data, they are convinced that the data are true or until the suspicions of money laundering or terrorist financing are eliminated.

14. OBLIGATION TO REPORT TO THE FINANCIAL INTELLIGENCE UNIT.

14.1. The Responsible Person must report to the Financial Intelligence Unit on (i) the activity or (ii) the circumstances that they identify in the course of economic activities and whereby:

14.1.1. the characteristics indicate the use of criminal proceeds or the commission of crimes related to this (this is primarily a report on a suspicious and unusual transaction or activity, i.e. Unusual

transaction report (UTR) or Unusual activity report (UAR));
14.1.2. in the case of which the Responsible Person suspects or knows or the characteristics of which indicate the commission of money laundering or related crimes (this is primarily a report on a transaction or activity whereby money laundering is suspected, i.e. Suspicious transaction report (STR) or Suspicious activity report (SAR));
14.1.3. in the case of which the Responsible Person suspect or know or the characteristics of which indicate the commission of terrorist financing or related crimes (this is primarily a report on a transaction or activity whereby terrorist financing is suspected, i.e. Terrorist financing report (TFR));
14.1.4. in the case of which an attempt of the activity or circumstances specified in points 14.1.1 to 14.1.3 of these Guidelines is present.

14.2. The Financial Intelligence Unit must be notified:

14.2.1. by the Responsible Person also about the circumstances of refusal of establishment of a business relationship or completing an occasional transaction on the basis of point 6.1.1 of these Guidelines and about the extraordinary termination of a business relationship on the basis of these Guidelines (primarily a suspicious and unusual transaction or activity report, i.e. UAR);
14.3. The reports specified in points 14.1 and 14.2 of these Guidelines must be made before the completion of the transaction if the Company suspects or knows that money laundering or terrorist financing or related crimes are being committed and if said circumstances are identified before the completion of the transaction. Considering the speed at which money laundering and terrorist financing crimes are committed, such performance of the obligation to report before the completion of the transaction may also be appropriate in other cases. If the postponement of the transaction may cause considerable harm, it is not possible to omit the transaction or it may impede capture of the person who committed possible money laundering or terrorist financing, the transaction will be concluded and a report will be submitted the Financial Intelligence Unit thereafter. The Responsible Person is in contact with the Financial Intelligence Unit in order to identify such circumstances.

14.4. In any case (i.e. also in the situation where an activity or circumstance is identified after the completion of the transaction), the reporting obligation must be performed immediately, but not later than two working days after the identification of the activity or circumstance or the emergence of the actual suspicion (i.e. the situation where the suspicion cannot be dispelled). The purpose of immediate reporting is to give the Financial Intelligence Unit the opportunity to have its own suspicions and apply its own measures, considering that money laundering is a process where criminal proceeds, especially financial assets, can be transferred through the financial institutions of several countries in one working day, which is why quick reporting helps trace black money more efficiently.

14.5. In addition to the situation specified in point 14.3 of these Guidelines, the Responsible Person must also wait for the feedback of the Financial Intelligence Unit in other appropriate cases before refusing to establish a business relationship or before the termination of a business relationship.

14.6. In a situation where, in the case of a socalled amountbased report or a report arising from the establishment or extraordinary termination of a business relationship and in respect of the Client or the circumstances related to them, the obliged entity has identified the activity or circumstances specified in point 14.1 of these Guidelines, the reporting obligation must also be performed within the meaning of point 14.1 of these Guidelines, whereby this may also take place within the scope of the same report, but by making reference to different indicators.

14.7. If the basis for compliance with the reporting obligation of the Company is not a suspicion of money laundering or terrorist financing, but a socalled suspicious or unusual transaction and there are

many such suspicious and unusual transactions and several reports have been made on the basis of these or the reports are continuing (and the making of such reports has not been extraordinarily agreed with the Financial Intelligence Unit), the Responsible Person must start suspecting money laundering or terrorist financing, after which other due diligence measures have to be applied in addition to the relevant report and the refusal to conclude a transaction must be decided.

14.8. Upon the performance of the reporting obligation related to the payment service, the obliged entity also decides whether it would also be appropriate to inform the Financial Intelligence Units of the other countries related to the payment about the payment and, if necessary does this or asks the Estonian Financial Intelligence Unit to make the relevant report.

15. OBLIGATION TO APPLY DUE DILIGENCE MEASURES AGAIN.

15.1. If necessary, the Compliance specialist will apply due diligence measures to existing clients again if they see that due diligence measures have not been adequately applied to existing clients in order to comply with the requirements set out in these Guidelines.
15.2. When assessing the need to apply due diligence measures, the Compliance specialist also proceeds from the Client's significance and risk profile and the time that has passed from the previous application of due diligence measures or the scope of their application.
15.3. The Compliance specialist reviews business relationships in order to identify whether one or several of the high risk characteristics specified these Guidelines, including all annexes, are present in the activities of their clients. The Compliance specialist takes the relevant measures, where necessary, to mitigate said risks.