Skrillnex OÜ

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

Tallinn
2020

1. GENERAL TERMS

1.1. These guidelines provide the internal rules of procedure and internal control rules for the company to perform due diligence obligations pursuant to Money Laundering and Terrorist Financing Prevention Act and International Sanctions Act.

1.2. The basis of these guidelines comprises International Sanctions Act (RSanS), Money Laundering and Terrorist Financing Prevention Act (RahaPTS) and Directive (EU) 2015/849 of the European Parliament and of the Council.

1.3. The purpose of these guidelines is, by increasing the trustworthiness and transparency of the business environment, to prevent the use of the financial system and economic space of the Republic of Estonia for money laundering and terrorist financing.

1.4. These guidelines regulate and provide:

1.4.1. the principles of assessment, management and mitigation of risks related to money laundering and terrorist financing;

1.4.2. the procedure for the application of due diligence measures regarding a customer, including a procedure for the application of simplified and enhanced due diligence measures;

1.4.3. the instructions for effectively identifying whether a person is a politically exposed person or a local politically exposed person or a person subject to international sanctions or a person whose place of residence or seat is in a high-risk third country;

1.4.4. the procedure for data collection, retention and making data available;

1.4.5. the model for identification and management of risks relating to a customer and its activities and the determination of the customer's risk profile;

1.4.6. the methodology and instructions where the obliged entity has a suspicion of money laundering and terrorist financing or where an unusual transaction or circumstance is involved as well as instructions for performing the reporting obligation and procedures for informing the management;

1.4.7. the procedure for identification and management of risks relating to new and existing technologies, and services and products, including new or non-traditional sales channels and new or emerging technologies.

1.5. The provisions of these guidelines apply to all business relationships and transactions related to customers, including transactions made through agents and the transfer of economic activities to a third party pursuant to the procedure provided by RahaPTS.

1.6. The management board of the legal person that is an obliged entity, the director of a branch that is an obliged entity or, upon their absence, the obliged entity must ensure that the employees whose employment duties include the establishment of business relationships or the making of transactions are provided with training in the performance of the duties and obligations arising from RahaPTS and such training must be provided when the employee commences performance of the specified employment duties, and thereafter regularly or when necessary. In training, information, inter alia, on the duties and obligations provided for in the rules of procedure, modern methods of money laundering and terrorist financing and the related risks, the personal data protection requirements, on how to recognise acts

related to possible money laundering or terrorist financing, and instructions for acting in such situations must be given.

1.7. The management board of the company is obliged to introduce these guidelines with appendices to all employees upon employment and thereafter as necessary, but not less than once per year.

1.8. The employees and the management board of the company are obliged to confirm the examination of these instructions with their handwritten signature.

1.9. The employees and the management board of the company are personally liable for the compliance with the requirements of the RahaPTS pursuant to the procedure provided by law.

1.10. A regular review is performed whether the rules of procedure are up to date and they will be supplemented and updated as necessary, but not less frequently than once per year.

1.11. The employees of the company must be familiar with and strictly follow the requirements provided for in the RahaPTS, the instructions for identifying the characteristics of a transaction suspected of money laundering and terrorist financing issued by the Financial Intelligence Unit and these guidelines.

1.12. The employees of the company must independently examine the amendments to laws and other legislation that appear on the website of the Financial Intelligence Unit https://www2.politsei.ee/et/organisatsioon/rahapesu/ but not less than once per year.

1.13. Obliged entities cooperate with one another and with state supervisory and law enforcement authorities in preventing money laundering and terrorist financing, including communicating information available to them and replying to queries within a reasonable time, following the duties, obligations and restrictions arising from legislation.

2. DEFINITIONS

2.1. **Company** – Skrillnex OÜ.

2.2. **Money laundering** means:

2.2.1. the conversion or transfer of property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions;

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

2.2.3. the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such

property is derived from criminal activity or from an act of participation in such an activity.

2.2.4. Money laundering also means participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the activities referred to in subsection 2.1.1. of this section.

2.2.5. Money laundering is regarded as such also where a criminal activity which generated the property to be laundered was carried out in the territory of another country.

2.2.6. Money laundering is regarded as such also where the details of a criminal activity which generated the property to be laundered have not been identified.

2.3. **Terrorist financing** means the financing and supporting of an act of terrorism and commissioning thereof as well as the financing and supporting of travel for the purpose of terrorism within the meaning of §§ 237^3 and 237^6 of the Penal Code.

2.4. **Financial Intelligence Unit** – independent structural unit of the Police and Border Guard Board which exercises supervision and applies enforcement powers on the state on the basis and pursuant to the procedure prescribed by law. Postal address: Tööstuse 52, 10416 Tallinn; e-mail: rahapesu@politsei.ee; phone (+372) 612 3840; fax: (+372) 612 3845.

2.5. **Cash** means cash within the meaning of Article 2(2) of Regulation (EC) No 1889/2005 of the European Parliament and of the Council on controls of cash entering or leaving the Community (OJ L 309, 25.11.2005, pp 9–12);

2.6. **Property** means any object as well as the right of ownership of such object or a document certifying the rights related to the object, including an electronic document, and the benefit received from such object;

2.7. **Obliged entity** means a person of the company specified in § 2 of rahaPTS, which include the following persons in the economic and professional activities:

2.7.1. credit institutions;

2.7.2. financial institutions;

2.7.3. gambling operators, except for organisers of commercial lotteries;

2.7.4. persons who mediate transactions involving the acquisition or the right of use of real estate; traders within the meaning of the Trading Act, where a cash payment of no less than 10,000 euros or an equal amount in another currency is made to or by the trader, regardless of whether the financial obligation is performed in the transaction in a lump sum or by way of several linked payments over a period of up to one year, unless otherwise provided by law;

2.7.5. persons engaged in buying-in or wholesale of precious metals, precious metal articles or precious stones, except precious metals and precious metal articles used for production, scientific or medical purposes;

2.7.6. auditors and providers of accounting services;

2.7.7. providers of accounting or tax advice services;

2.7.8. providers of trust and company services;

2.7.9. providers of a virtual currency service;

2.7.10. a central securities depository where it arranges the opening of securities accounts and provides services related to register entries without the mediation of an account operator;

2.7.11. undertakings providing a cross-border cash and securities transportation service;

2.7.12. pawnbrokers.

2.8. **Business relationship** means a relationship that is established upon conclusion of a long-term contract by an obliged entity in economic or professional activities for the purpose of provision of a service or sale of goods or distribution thereof in another manner or that is not based on a long-term contract, but whereby a certain duration could be reasonably expected at the time of establishment of the contact and during which the obliged entity repeatedly makes separate transactions in the course of economic or professional activities while providing a service or professional service, performing professional acts or offering goods;

2.9. **Customer** means a person who has a business relationship with an obliged entity;

2.10. **Financial institution** means:

2.10.1. a foreign exchange service provider;

2.10.2. a payment service provider within the meaning of the Payment Institutions and E-money Institutions Act, except for a payment initiation service provider and an account information service provider;

2.10.3. an e-money institution within the meaning of the Payment Institutions and E-money Institutions Act;

2.10.4. an insurance undertaking within the meaning of the Insurance Activities Act (hereinafter *insurance undertaking*) to the extent that it provides services related to life insurance, except for services related to mandatory funded pension insurance contracts within the meaning of the Funded Pensions Act;

2.10.5. an insurance broker within the meaning of the Insurance Activities Act (hereinafter *insurance broker*) to the extent that it is engaged in marketing life insurance or provides other instrument-related services;

2.10.6. a management company, except upon managing a mandatory pension fund within the meaning of the Funded Pensions Act, and an investment fund founded as a public limited company within the meaning of the Investment Funds Act;

2.10.7. an investment firm within the meaning of the Securities Market Act;

2.10.8. a creditor and a credit intermediary within the meaning of the Creditors and Credit Intermediaries Act;

2.10.9. a savings and loan association within the meaning of the Savings and Loan Associations Act;

2.10.10. a central contact point designated by an e-money institution or a payment service provider;

2.10.11. another financial institution within the meaning of the Credit Institutions Act;

2.10.12. provider of a virtual currency service.

2.11. **Precious stones** means natural and artificial precious stones and semi-precious stones, their powder and dust, and natural and cultivated pearls;

2.12. **Precious metal** means precious metal within the meaning of the Precious Metal Articles Act;

2.13. **Precious metal article** means a precious metal article within the meaning of the Precious Metal Articles Act;

2.14. **Virtual currency** means a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal 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, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, pp. 35–127) or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same Directive;

2.15. **Virtual currency exchange service** means a service with the help of which a person exchanges a virtual currency against a fiat currency or a fiat currency against a virtual currency or a virtual currency against another virtual currency;

2.16. **Virtual currency wallet service** means a service in the framework of which keys are generated for customers or customers' encrypted keys are kept, which can be used for the purpose of keeping, storing and transferring virtual currencies;

2.17. **Virtual currency service** means a service specified in clauses 2.15 or 2.16.

2.18. **Foreign exchange services** means the exchanging of a valid currency against another valid currency by an undertaking in its economic or professional activities;

2.19. **Group** means a group of undertakings which consists of a parent undertaking, its subsidiaries within the meaning of § 6 of the Commercial Code, and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings that constitute a consolidation group for the purposes of subsection 3 of § 27 of the Accounting Act;

2.20. **International sanctions** means an essential tool of foreign policy aimed at supporting the maintenance or restoration of peace, international security, democracy and the rule of law, following human rights and international law or achieving other objectives of the United Nations Charter or the Common Foreign and Security Policy of the European Union.

2.21. **High-risk third country** means a country specified in a delegated act adopted on the basis of Article 9(2) of Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141/73, 05.06.2015, pp 73–117).

2.22. **Compliance officer** means an employee appointed by the resolution of the management board of the company who shall act as the compliance officer for the Financial Intelligence Unit and who regulates and supervises the fulfilment of measures for the prevention of money laundering and terrorist financing. If no specific compliance officer has been appointed by the resolution of the management board, the obligations of the compliance officer shall be fulfilled by the member of the management board of the legal entity.

3. PRINCIPLES OF OBLIGED ENTITY'S RISK MANAGEMENT

3.1. The obliged entity shall regularly prepare and update the risk assessment in order to identify, assess and analyse the risks of money laundering and terrorist financing related to its activities.

3.2. The obliged entity identifies the risks/threats associated with its activities, as well as the risks/threats that may arise in the near future, that is foreseeable risks/threats, and assesses and analyses their significance and impact. The risks/threats are identified and assessed on a case-by-case basis as of the moment of the risk assessment and separately considering the situation where the obliged entity should take the risks to the maximum extent permitted by the risk appetite. The obliged entity identifies, assesses and analyses at least the following risks:

3.2.1. risks relating to customers;

3.2.2. risks relating to products, services or transactions, including risks relating to new and/or future products, services or transactions:

3.2.3. risks relating to communication, mediation or products, services, transactions or delivery channels between the obliged entity and customers including if the abovementioned is new and/or provided in the future;

3.2.4. risks relating to countries, geographic areas or jurisdictions.

3.3. The company identifies risk factors for the risks specified in clauses 3.2.1-3.2.4 that increase or decrease the risk of money laundering and terrorist financing.

3.4. As a result of the risk assessment, the obliged entity establishes:

3.4.1. the risk factors which may affect the risk;

3.4.2. the risk appetite, including the volume and scope of products and services provided in the course of business activities;

3.4.3. the risk management model, including simplified and enhanced due diligence measures, in order to mitigate identified risks.

3.5. The risk assessment and the establishment of the risk appetite is documented, the documents are updated where necessary and based on the published results of the national risk assessment. At the request of the competent supervisory authority, the obliged entity submits the prepared documents to the supervisory authority.

3.6. The obliged entity shall update or renew the risk assessment and the related documents when necessary, but not less than once per year.

4. PRINCIPLES FOR STRUCTURE OF OBLIGED ENTITY'S ORGANISATION

4.1. The organisational structure of the obliged entity must correspond to its size and the nature, scope and level of complexity of the activities and services provided, including the risk appetite and related risks, and must be structured following the principle of so-called three lines of defence. The organisational structure of the obliged entity corresponds to the complete understanding of potential risks and their management. The reporting and subordination chains of the obliged entity must be ensured in such a way that all employees know their place in the organisational structure and know their work duties.

4.2. The management board of the obliged entity is the carrier of the culture of compliance with the requirements of money laundering and terrorist financing prevention, guaranteeing that the managers and employees of the obliged entity operate in an environment where they are fully aware of the requirements for the prevention of money laundering and terrorist financing and the obligations associated with these, and the relevant risk considerations are taken into account to a suitable extent in the decision-making processes of the obliged entity.

4.3. The employees of the obliged entity must act with the foresight and competence expected from them and according to the requirements set for their positions, proceeding from the interests and the goals of the obliged entity, and ensure that the Estonian financial system and economic space are not used for money laundering and terrorist financing. The obliged entity takes measures to assess the suitability of the employees before they start working.

4.4. The organisational structure of the obliged entity for the purposes of the risk management matrix is built by the three lines of defence principle, where each line of defence has a separate task with the goal to prevent money laundering and terrorist financing and each line of defence has certain independence and adequate resources for an effective operation.

4.5. **The first line of defence** has the function of applying due diligence measures upon business relationship and one-off transactions and applying due diligence measures during the business relationship. First line of defence comprises the structural units and employees of the obliged entity with whose activities risks are associated and that must identify and assess these risks, their specific features and scope and that manage these risks by way of their ordinary activities, primarily by way of application of due diligence measures. The risks arising from the activities of and provision of services by the obliged entity belong to the first line of defence. They are the managers (owners) of these risks and responsible for them.

4.5.1. The first line of defence must have good knowledge of the customer and the specific features of their activities and business activities. This way, the employees in the first line of defence must be aware of or make themselves aware of the specific features of the different business activities of customers and the risks associated with them if the obliged entity has decided to provide services to such customers. The goal is to identify transactions in the customer's activities that are suspicious or unusual or do not correspond to reasonable economic objectives, or transactions that refer to such circumstances, so they can be referred to the second line of defence for analysis.

4.5.2. First line of defence primarily comprises all employees who have the right to make transactions on behalf of the obliged entity. When explaining work tasks to the employee, the obliged entity notifies the person whether he or she is part of the first line of defence.

4.6. **The second line of defence** consists of the risk management and compliance functions. These functions may also be performed by the same person or structural unit depending on the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and risks arising from activities of the obliged entity.

4.6.1. The objective of the compliance function is to guarantee that the obliged entity complies with effective legislation, guidelines and other documents and to assess the possible effect of any changes in the legal or regulative environment on the activities of the obliged entity and on the compliance framework.

4.6.2. The task of compliance is to help the first line of defence as the owners of risk to define the places where risks manifest themselves (e.g. analysis of suspicious and unusual transactions, for which compliance employees have the required professional skills, personal qualities, etc.) and to help the first line of defence manage these risks efficiently. The second line of defence does not engage in taking risks.

4.6.3. Risk policy is implemented and the risk management framework is controlled via the risk management function. The performer of the risk management function ensures that all risks are identified, assessed, measured, monitored and managed, and informs the appropriate units of the obliged entity about them. The performer of the risk management function for the purposes of money laundering and terrorist financing prevention primarily performs the supervision over adherence to risk appetite, supervision over risk tolerance, supervision over identification of changes in risks, performs the overview of associated risks, and performs other duties related to risk management.

4.6.4. The compliance and risk control employees involved in the prevention of money laundering and terrorist financing (if they are not parts of the function of the compliance officer of the Financial Intelligence Unit) must also comply with the same requirements set for the compliance officer of the Financial Intelligence Unit.

4.7. **The third line of defence** is comprised by the independent and effective internal audit function. The internal audit function may be performed by one or several employees and/or a structural unit with the relevant functions. In the case of a structural unit, the entire unit must comply with the requirements set out below and the head of the structural unit is responsible for the performance of the functions.

4.7.1. The person who performs the internal audit function must have the required competency, tools and access to the relevant information in all structural units of the obliged entity. The performer of the internal audit function must also be aware of the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and risks arising from activities of the obliged entity.

4.7.2. The person who performs the internal audit function or their head if it is a structural unit must have the relevant professional standard (attestation) for the performance of their duties and, among others, the required education,

suitability, necessary capabilities, personal qualities, knowledge and experience, and impeccable professional and business reputation. The person who performs the internal audit function must always be informed about the risks and trends of money laundering and terrorist financing both at the general level and in the context of the obliged entity.

4.7.3. The internal audit methods must comply with the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and risks arising from activities of the obliged entity. This means that the regularity of carrying out audits and the assessed areas must take into account the circumstances specified in this point. The internal audit also proceeds from the risk-based and proportionality principle.

4.7.4. The internal audit function can be outsourced to a third person. The obliged entity constantly assesses whether outsourcing the internal audit function is justified and the efficiency of the internal audit.

4.8. The decision to conduct an internal audit is made by a resolution of the management board of the obliged entity. The management board must regularly assess the need to conduct an internal audit.

5. ACTIVITIES OF MANAGEMENT BOARD

5.1. The management board of the obliged entity must act with the foresight and competence expected from it and according to the requirements set forth, proceeding from the interests of the obliged entity and its customers, and ensure that the Estonian financial system and economic space are not used for money laundering and terrorist financing.

5.2. The management board of the obliged entity must determine the risk appetite of the obliged entity. In order to do this, the management board of the obliged entity, among others:

5.2.1. guarantees the preparation of risk appetite and risk assessment documents and their regular reviews and updates;

5.2.2. guarantees risk management measures for assessment of compliance with the risk appetite document and identification of associated changes in risks within reasonable time. The management board of the obliged entity or the responsible person(s) appointed at the level of management board immediately take measures upon the emergence of a deviation and change the organisational solution accordingly and, if necessary, suspend the provision of services in the relevant part in full or in part until the organisational solution has been changed.

5.3. The management board of the obliged entity must establish and regularly review the principles and procedures related to the taking, management, monitoring and mitigation of risks related to money laundering and terrorist financing, which cover both existing and potential risks. The management board of the obliged entity must also constantly determine and assess all of the money laundering and terrorist financing risks arising from the activities and guarantee the monitoring and inspection of their size, thereby also guaranteeing the existence of adequate staff and other compensation mechanisms required for risk management. In order to do this, the management board of the obliged entity, among others:

5.3.1. is constantly aware of the risks/threats that the obliged entity encounters in the course of economic activities. For this purpose, the management board of the obliged entity receives regular overviews of associated risks and the organisation's resilience, and trains itself (or at least the responsible member of the management board) in order to obtain an overview of new money laundering and terrorist financing trends, updated legislation or international practice or the guidelines of Finantsinspektsioon and other documents;

5.3.2. establishes rules of procedure for compliance with the RahaPTS and the legislative acts directly related thereto and guarantees that the employees directly involved in compliance with the requirements of the RahaPTS and this document act in conditions where they are fully aware of the requirements of the RahaPTS and this document;

5.3.3. establishes an organisational solution (incl. with the relevant IT capacity) and includes adequate human resources to ensure the compliance thereof with the maximum permitted risk appetite and capability thereof to withstand and mitigate the risks/threats associated with this maximum risk appetite. The obliged entity may decide to carry out stress tests to ascertain the compensation mechanisms to be used as cover for the maximum permitted risks. If the management board of the obliged entity is not prepared to establish an organisational solution that complies with the size of the permitted maximum risk appetite and the associated risks/threats, the management board of the obliged entity must establish an organisational solution and include adequate quantities of human resources that comply with the size of the risks taken at all times. In such a case the management board of the obliged entity will also create an solution that assesses the scale of the associated risks after short intervals of time and assesses the adequacy of the organisational solution for the risks taken, and in the case of a conflict responds immediately by supplementing the relevant organisation and decides, where necessary, not to take any additional risks and/or reduce the existing risks until the establishment of the relevant solution;

5.3.4. in addition to the creation of an organisational solution and the allocation of adequate human resources, ensures that the functional separation of different lines of defence and management of conflicts of interest are guaranteed. This obligation calls for, among others, regular assessment of whether the bases for remuneration of managers and employees, incl. economic interests in respect of third parties, will motivate them to waive or make concessions in compliance with the provisions of legislation and the Guidelines. The management board guarantees solution for identification, assessment, management and reduction of compliance or non-compliance with the aforementioned principles;

5.3.5. guarantees that the person(s) appointed by them ensures (ensure) compliance with due diligence measures according to the provisions of legislation and the recommendations made in these guidelines, and makes sure that the implemented measures are appropriate, correspond to the activity profile of the service provider and are in accordance with the customer, the nature, size and scope of the transaction as well as the associated money laundering or terrorist financing risks.

5.4. The management board of the obliged entity must organise the effective functioning of the internal control system and ensure control that the activities of the obliged entity, their managers and employees comply with legislation and the documents approved by the managing bodies as well as good practices. The management board of the obliged entity thereby regularly assesses the efficiency of the internal procedures implemented for compliance with the RahaPTS and rules of procedure and ensures internal control of such compliance.

5.5. The obliged entity appoints the person(s) who is (are) responsible for performance of the obligations stipulated in the RahaPTS at the level of the management board. Whereby:

5.5.1. the competency and responsibility of said person must arise from the internal documents that regulate the duties of members of the management board in a manner that is transparent and unambiguous;

5.5.2. only a person who has the appropriate knowledge, skills, experience and education on money laundering and terrorist financing prevention, is professionally suitable and has an impeccable business reputation may be elected or appointed the responsible member of the management board. The responsible member of the management board is constantly aware of the risks that affect the obliged entity and of the organisational solution that is capable of mitigating specific risks. A manager must demonstrate sufficient professionalism, integrity, accuracy and diligence in their activities to ensure the compliance with the requirements for prevention of money laundering and terrorist financing.

5.6. The management board of the obliged entity retains data in a form that can be reproduced in writing of the decision-making process with which it performs the measures implemented upon the assumption of the obligations specified in this sub-chapter, the measures taken for implementation and other measures taken for the prevention of money laundering and terrorist financing.

6. COMPLIANCE OFFICER

6.1. Where the obliged entity has more than one management board member, the obliged entity appoints a management board member who is in charge of implementation of RahaPTS and legislation and guidelines adopted on the basis thereof.

6.2. The management board of a credit institution and financial institution and the director of the branch of a foreign credit institution and financial institution registered in the Estonian commercial register appoint a person who acts as the compliance officer of the Financial Intelligence Unit. The compliance officer of the credit institution or financial institution reports directly to the management board of the credit institution or financial institution and has the competence, means and access to relevant information across all the structural units of the credit institution or financial institution.

6.3. The obliged entity who is not a credit institution or financial institution may appoint a compliance officer for the performance of prevention of money laundering and terrorist financing duties and obligations. Where no compliance officer has been appointed, the duties of a compliance officer are performed by the management

board of the legal person, the appointed management board member, the director of the branch of the foreign company registered in the Estonian commercial register or a sole proprietor.

6.4. An employee or a structural unit may perform the duties of a compliance officer. Where a structural unit performs the duties of a compliance officer, the head of the respective structural unit is responsible for performance of the given duties. The Financial Intelligence Unit and the competent supervisory authority are informed of the appointment of a compliance officer.

6.5. Only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties of a compliance officer may be appointed as a compliance officer. The appointment of a compliance officer is coordinated with the Financial Intelligence Unit.

6.6. The duties of a compliance officer include, inter alia:

6.6.1. organisation of the collection and analysis of information referring to unusual transactions or transactions or circumstances suspected of money laundering or terrorist financing, which have become evident in the activities of the obliged entity;

6.6.2. reporting to the Financial Intelligence Unit in the event of suspicion of money laundering or terrorist financing;

6.6.3. periodic submission of written statements on compliance with the requirements arising from this Act to the management board of a credit institution or financial institution or to the director of the branch of a foreign credit institution or financial institution registered in the Estonian commercial register;

6.6.4. performance of other duties and obligations related to compliance with the requirements of RahaPTS.

6.7. A compliance officer has the right to:

6.7.1. make proposals to the management board of a credit or financial institution or to the director of the branch of a foreign credit or financial institution registered in the Estonian commercial register for amendment and modification of the rules of procedure containing the requirements of prevention of money laundering and terrorist financing and organisation of training specified in subsection 6 of § 14 of RahaPTS;

6.7.2. receive data and information required for performance of the duties of a compliance officer;

6.7.3. make proposals for organisation of the process of submission of notifications of suspicious and unusual transactions;

6.7.4. demand that a structural unit of the obliged entity eliminate within a reasonable time deficiencies identified in the implementation of the requirements of prevention of money laundering and terrorist financing;

6.7.5. receive training in the field.

6.8. The compliance officer may deliver information or data which has become known to him or her in connection with a suspicion of money laundering only to:

6.8.1. the Financial Intelligence Unit;

6.8.2. a pre-trial investigation authority in connection with criminal proceedings;

6.8.3. the court on the basis of a court order or decision.

6.9. Each employee of the company must inform the compliance officer of all cases of refusal to establish a business relationship on the basis of RahaPTS, suspicious or unusual transactions, cases of extraordinary termination of the long-term contract and other circumstances that may affect the performance of the obligations of the obliged entity under RahaPTS.

6.10. If during the course of an economic or professional activity or official activity the employee identifies an activity or circumstances the characteristics of which indicate money laundering or terrorist financing or which the employee suspects or knows is money laundering or terrorist financing, he or she shall immediately inform the compliance officer. If identifying suspicious transactions, the employee relies among other things on the guidelines on indications suspected of money laundering and the guidelines on suspected terrorist financing transactions issued by the Financial Intelligence Unit.

7. GENERAL CRITERIA FOR APPLICATION OF DUE DILIGENCE MEASURES

7.1. Applied due diligence measures regarding a customer are:

7.1.1. identification of a customer or a person participating in an occasional transaction and verification of 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;

7.1.2. identification and verification of a representative of a customer or a person participating in an occasional transaction and their right of representation;

7.1.3. identification of the beneficial owner and, for the purpose of verifying their identity, taking measures to the extent that allows the obliged entity to make certain that they know who the beneficial owner is, and understands the ownership and control structure of the customer or of the person participating in an occasional transaction;

7.1.4. understanding of business relationship or an occasional transaction or act and, where relevant, gathering additional information thereof;

7.1.5. gathering information on whether a person is a politically exposed person, their family member or a person known to be a close associate;

7.1.6. business relationship monitoring.

7.2. The obliged entity has applied due diligence measures adequately if the obliged entity has the inner conviction that they have complied with the obligation to apply due diligence measures. The principle of reasonability is observed in the consideration of inner conviction. This means that the obliged entity must, upon the application of due diligence measures, acquire the knowledge, understanding and assertation that they have collected enough information about the customer, the customer's activities, the purpose of the business relationship and of the transactions carried out within the scope of the business relationship, the origin of the funds, etc., so that they understand the customer and customer's (business) activities, thereby taking into account the customer's risk level, the risk associated with the business relationship and the nature of such relationship. Such a level of assertation must make it possible to identify complicated, high-value and unusual transactions and transaction patterns that have no reasonable or obvious economic

or legitimate purpose or are uncharacteristic of the specific features of the business in question

7.3. When applying clause 7.1.4, the obliged entity must understand the objective of the business relationship or the occasional transactions, determining, among other things, the permanent place of business, place of activity or place of residence of the customer or of the person participating in an occasional transaction, their professional or business field, important transaction partners, payment practices and, in case of a legal person, their prior experience.

7.4. Upon the demand of the obliged entity, the person or customer participating in a transaction made during the economic or professional activities submits the documents and provides the information required for the purposes of applying due diligence measures provided for in subclauses 1-5 of clause 7.1. Upon the demand of the obliged entity, the person or customer participating in a transaction made during the economic or professional activities confirms with their signature that the information and documents submitted for the application of the due diligence measures are true.

7.5. The due diligence measures provided for in subclauses 1-5 of clause 7.1 **must be applied before establishing the business relationship or, if not in business relationship, before the transaction.**

7.6. Due diligence measures are applied by the obliged entity:

7.6.1. upon establishment of a business relationship and ongoing monitoring of the business relationship;

7.6.2. upon executing or mediating occasional transactions outside a business relationship where the value of the transaction exceeds 15 000 euros or an equal amount in another currency, regardless of whether the financial obligation is performed in the transaction in a lump sum or in several linked payments over a period of up to one year, unless otherwise provided by law. Due diligence measures must thereby be applied as soon as the exceeding of the sum becomes known or, where the exceeding of the sum depends on the making of several linked payments, as soon as the sum is exceeded;

7.6.3. 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;

7.6.4. upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or thresholds provided by law.

7.7. If necessary, the obliged entity will apply due diligence measures to existing customers again if they see that due diligence measures have not been adequately applied to existing customers in order to comply with the requirements set out in these guidelines. When assessing the need to apply due diligence measures, the obliged entity also proceeds from the customer'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.

7.8. The application of due diligence measures is the responsibility of the employee of the obliged entity who performs the transaction on behalf of the obliged entity. In all other cases, the due diligence measures of the obliged entity shall be the responsibility of the highest management body of the obliged entity.

8. SIMPLIFIED DUE DILIGENCE MEASURES

8.1. The obliged entity may apply simplified due diligence measures if they have identified according to the risk assessment prepared by the obliged entity that in the case of the economic or professional activity, field or factors, the risk of money laundering or terrorist financing is lower than usual.

8.2. Before the application of simplified due diligence measures to a customer, the obliged entity establishes that the business relationship, transaction or act is of a lower risk.

8.3. The application of simplified due diligence measures is permitted to the extent that the obliged entity ensures sufficient monitoring of transactions, acts and business relationships, so that it would be possible to identify unusual transactions and allow for notifying of suspicious transactions in accordance with the procedure established in § 49 of RahaPTS.

8.4. Upon simplified implementation of due diligence measures, the identity of a customer or of the customer's representative may be verified on the basis of information obtained from a credible and independent source also at the time of establishment of the business relationship, provided that it is necessary for not disturbing the ordinary course of business. In such an event the verification of identity must be carried out as quickly as possible and before the taking of binding measures.

8.5. Upon simplified implementation, the obliged entity may choose the extent of performance of the duty and the need to verify the information and data used therefore with the help of a credible and independent source.

8.6. Due diligence measures may be applied in accordance with the simplified procedure, provided that a factor characterising a lower risk has been established and ay least the following criteria are met:

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

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

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

8.7. Simplified due diligence measures in establishing business relationship and executing occasional transactions include, among other things:

8.7.1. verifying the identity of a customer or of the customer's representative on the basis of information obtained from a credible and independent source also at the time of establishment of the business relationship, provided that it is necessary for not disturbing the ordinary course of business.

8.7.2. assuming the nature and purpose of the business relationship, because the product has been created for one specific purpose only;

8.7.3. obtaining information from the customer when the beneficial owner is checked, not from an independent source.

8.8. Simplified due diligence measures in business relationship monitoring include, among other things:

8.8.1. adjustment of the frequency of updating and review of the due diligence measures implemented in respect of a customer in a business relationship, e.g. by only doing so if a certain trigger event occurs (however, this may not lead to avoidance of the obligation to update or monitor data);

8.8.2. adjustment of the frequency and intensity of transaction monitoring, e.g. by only monitoring transactions that have exceeded a certain threshold (the threshold must be set at a reasonable level and the identification of related transactions must be ensured).

8.9. The obliged entity documents and, upon the demand of the supervisory authority, demonstrates why, in respect of what and which simplified due diligence measures the obliged entity has applied to the customer upon the establishment of the business relationship or in respect of transactions during the business relationship.

9. ENHANCED DUE DILIGENCE MEASURES

9.1. The obliged entity applies enhanced due diligence measures in order to adequately manage and mitigate a higher-than-usual risk of money laundering and terrorist financing.

9.2. Enhanced due diligence measures are applied always when:

9.2.1. upon identification of a person or verification of submitted information, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;

9.2.2. the person participating in the transaction or professional act made in economic or professional activities, the person using the professional service or the customer is a politically exposed person, except for a local politically exposed person, their family member or a close associate;

9.2.3. the customer participating in the transaction made in economic or professional activities is from a high-risk third country or their place of residence or seat or the seat of the payment service provider of the payee is in a high-risk third country;

9.2.4. the customer or the person participating in the transaction is from such country or territory or their place of residence or seat or the seat of the payment service provider of the payee is in a country or territory that, according to credible sources such as mutual evaluations, reports or published follow-up reports, has not established effective AML/CFT systems that are in accordance with the recommendations of the Financial Action Task Force, or that is considered a low tax rate territory;

9.2.5. a complex, high-value or unusual transaction or transaction pattern takes place that does not have a reasonable or apparent economic or legitimate purpose or is not characteristic to a particular business field.

9.3. The obliged entity applies enhanced due diligence measures also where a risk assessment prepared by the obliged entity identifies that, in the case of the economic or professional activity, field or factors, the risk of money laundering or terrorist financing is higher than usual.

9.4. Enhanced due diligence measures do not need to be applied regarding the branch of an obliged entity established in a contracting state of the European Economic Area or a majority-owned subsidiary seated in a high-risk third country, provided that the branch and the majority-owned subsidiary fully comply with the group-wide procedures and the obliged entity assesses that the waiver to apply enhanced due diligence measures does not entail major additional risks of money laundering and terrorist financing.

9.5. Enhanced due diligence measures in business relationship monitoring include, among other things:

9.5.1. identification of all beneficial owners of the company, incl. those whose shareholding is below 25%;

9.5.2. carrying out an independent assessment of the customer and, if necessary, obtaining the approval of the senior management about new and existing customers on the basis of risk sensitivity;

9.5.3. identification of the reasons and circumstances why the customer uses complicated ownership structures and/or has registered the company in the specific country;

9.5.4. obtaining information about the source and/or origin of the wealth of the customer and their beneficial owner.

9.6. Enhanced due diligence measures in business relationship monitoring include, among other things:

9.6.1. 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;

9.6.2. 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 (e.g. the existence of customs documents, goods insurance contracts, confirmations of payment of customs duties, special equipment (refrigeration equipment), etc.).

9.7. The obliged entity documents and, upon the demand of the supervisory authority, demonstrates why, in respect of what and which enhanced due diligence measures the obliged entity has applied to the customer upon the establishment of the business relationship or in respect of transactions during the business relationship.

10. ADDITIONAL DUE DILIGENCE MEASURES

10.1. The obliged entity applies additional due diligence measures in order to manage and mitigate an established risk of money laundering and terrorist financing that is higher than usual, by choosing at their own discretion one or several due diligence measures of the following:

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

10.1.2. 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;

10.1.3. 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;

10.1.4. 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;

10.1.5. 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;

10.1.6. the application of due diligence measures regarding the person or their representative while being at the same place as the person or their representative.

10.2. 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.

10.3. The obliged entity documents and, upon the demand of the supervisory authority, demonstrates why, in respect of what and which additional due diligence measures the obliged entity has applied to the customer upon the establishment of the business relationship or in respect of transactions during the business relationship.

11. GENERAL PRINCIPLES OF IDENTIFICATION

11.1. If there is no obligation of applying due diligence measures, the obliged entity must acquire at least the following information from the customer:

11.1.1. customer's name;

11.1.2. in case of a natural person – their personal identification code, if not available, their place and time of birth and their place of residence or seat;

11.1.3. in case of a legal person and legal arrangement – name of its director and information confirming their right of representation, registry code, or other relevant registry number and registry date of the person;

11.1.4. objective of the transaction.

11.2. The obliged entity must ensure the correctness of data provided for by the clause 11.1.

11.3. Making transactions with or establishing a business relationship with a person who has not disclosed information provided for in clause 11.1, **is prohibited.**

11.4. The customer confirms the correctness of the information provided with their handwritten signature.

11.5. Simplified identification measures are applied when identifying a natural person permanently residing in Estonia or in a contracting state of the European Economic Area.

11.6. Before entering into a customer relationship with a politically exposed person, with a family member of a politically exposed person or with a person known to be close associate of a politically exposed person, the employee must acquire a permission from the management who shall decide on the purposefulness of the establishment of the customer relationship and gives instructions for the monitoring of the further customer relationship.

11.7. Before entering into a customer relationship with a legal person whose beneficial owner is a politically exposed person, a family member of a politically exposed person or a person known to be close associate of a politically exposed person in a contracting state of the European Economic Area or in a third country, the employee must acquire a permission from the management who shall decide on the purposefulness of the establishment of the customer relationship and gives instructions for the monitoring of the further customer relationship.

11.8. Before entering into a customer relationship with a legal person where there is a suspicion that its activity, persons entitled to represent it, or its beneficial owners, may be related to money laundering or terrorist financing, the employee must acquire a permission from the management who shall decide on the purposefulness of the establishment of the customer relationship and gives instructions for the monitoring of the further customer relationship.

11.9. If there is a justified suspicion when identifying a person that they are not acting on their own behalf or account, the employee shall identify the person whose behalf or account they are acting on.

11.10. If it is impossible to identify a person whose name or account the other person is acting on, the employee is prohibited to conclude a transaction with them. The employee is also obligated to inform the Financial Intelligence Unit of this person's declaration of intent to make a transaction or of a transaction that has already been made.

11.11. When first using the provided service or when establishing a business relationship, it is recommended to identify the person while being at the same place as the person.

11.12. If the employee becomes suspicious of the identification of the customer, the employee is obligated to ask for an additional document with a photograph for identification which makes it possible to verify the correctness of the identification.

11.13. When there is a suspicion of a document indicating forgery, it is recommended to keep the document, call the police and give the suspicious document to them. If possible, use the help of a security officer or other citizens. Such an event must be sent as a notification to the FIU.

11.14. The employee of the company shall determine the purpose and nature of the transaction and the business relationship.

11.15. The employee of the company is prohibited to make a transaction or enter into a contract with a person who refuses to provide the data provided for in the previous clause, as well as with a person who the employee suspects is acting as a front; when

the customer does not provide the required documents and the relevant information or when the employee becomes suspicious on the basis of the provided documents that there may be an event of money laundering or terrorist financing.

11.16. The information regarding the events provided for in clause 10.3 of these guidelines must be immediately delivered to the compliance officer of the Financial Intelligence Unit (the management board of the company) and to record as much customer information as possible that later helps to identify the customer.

11.17. The employee of the company shall apply these rules of procedure every time **before** making a occasional transaction or establishing a business relationship with a customer.

12. VERIFICATION OF INFORMATION OBTAINED DURING IDENTIFICATION

12.1. 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 to be.

12.2. A **credit institution** and a **financial institution** must identify a person and verify data with the help of information technology (hereinafter – IT) means where a business relationship is established with an e-resident or a person from the state outside of the European Economic Area or whose place of residence or seat is in such a country or with a person from a contracting state of the European Economic Area or whose place of residence or seat is in such a country and whose total sum of outgoing payments relating to a transaction or a service contract exceeds 15,000 euros per calendar month in the case of a customer who is a natural person or, in the case of a customer who is a legal person, 25,000 euros per calendar month, and where the due diligence measures are not applied while being physically in the same place as the person or their representative.

12.3. The information obtained during identification must be verified based on information obtained from a reliable and independent source.

12.4. The face-to-face identification or identification with an IT device 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.

12.4.1. Face-to-face identification means that the customer or their representative and the representative of the obliged entity are in the same place within the scope of a specific meeting. This means that the potential customer or their representative has direct contact with the representatives of the obliged entity in the course of which the obliged entity verifies from the reliable and independent source by comparing the person's biometrics (facial image) with the facial image on or obtained from the document specified in clause 14.3. Direct contact requires direct communication between the representative of the obliged entity and the customer or their representative to assess the compliance of the content of their

declaration of intent and goal with the actual intent. The experience obtained in the course of the direct contact makes it possible to determine the customer's risk level more accurately. The contact may take place outside the permanent place of business of the obliged entity if at least the same due diligence obligations that are performed in ordinary cases are performed in its course.

12.5. In situations not specified in clause 12.4, the reliable and independent source (must exist cumulatively) is verification of the information obtained in the course of identification, (a) which originates from two different sources, (b) where, if the money laundering and terrorist financing risk of the customer and the business relationship is average or higher than usual, the customer sends a photo taken of the facial image of the person for the specific financial service immediately before the data are sent and the obliged entity makes sure that the photo was taken recently and (c) which corresponds to the following features, i.e. reliable and independent source is information:

12.5.1. which has been issued by (identity documents) or received from a third party or a place that has no interest in or connections with the customer or the obliged entity, i.e. that is neutral (e.g. information obtained from the Internet is not such information, as it often originates from the customer themselves or its reliability and independence cannot be verified);

12.5.2. the reliability and independence of which can be determined without objective obstacles and reliability and independence are also understandable to a third party not involved in the business relationship; and

12.5.3. the data included in which or obtained via which are up to date and relevant and the obliged entity can obtain reassurance about this (and reassurance can in certain cases also be obtained on the basis of the two aforementioned clauses).

12.6. Irrespective of the selected reliable and independent source, the obliged entity must make sure in the case of identity documents that the document is valid and complies with the requirements stipulated in the Identity Documents Act and the person resembles the person depicted on the document photo in terms of appearance and age and the data included in the document.

12.7. Detailed instructions regarding the application of the contents of clause 12.5 (a) is provided for in the following sections.

12.8. The obliged entity is prepared, if necessary, to explain the selection of the identification measure and the verification measure to supervisory authority, incl. demonstrate why the source is reliable and independent, what the two different sources are (if two sources are used) and justify why the selected measure complies with the risk profile and risk level of the customer and the business relationship with the customer.

13. IDENTIFICATION OF PERSON USING INFORMATION TECHNOLOGY MEANS

13.1. When using information technology means to identify the person and to verify the person's identity data, the natural person or the legal representative of a legal person prescribed in subsections § 31 (1) and (2) of the RahaPTS, who wants to establish a business relationship or conclude an occasional transaction, must use the following:

13.1.1. a document issued on the basis of the Identity Documents Act for digital identification of a person or another electronic identification system with assurance level 'high' which has been added to the list published in the Official Journal of the European Union based on Article 9 of Regulation (EC) 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 repealing Directive 1999/93/EC (OJ L 257, 28.08.2014, pp 73–114) is used for identification of a person and verification of data with the help of information technology means;

13.1.2. an information technology tool with a working camera, microphone and necessary hardware and software for digital identification, as well as internet connection with adequate speed.

13.2. Tools provided for in clause 13.1.2 must meet the following requirements:

13.2.1. the information system must allow for digital identification of a person and digital signing;

13.2.2. the obliged person must verify the quality of its own and, if possible, the customer's information flow and ensure that the transmission of clear, recordable and reproducible synchronised sound and image, which is sufficient to understand the transmitted content unambiguously and reliably, is guaranteed;

13.2.3. the information flow containing image and sound is transmitted in real time;

13.2.4. the information flow that contains image and sound must be recorded with the time stamp, the customer's IP address, the personal identification code of the person to be identified, if there is no personal identification code, then the birth date and place and country of residence, whilst the time stamp must be tied to the data concerning it in such a manner that any later changes in data, the person who made the changes, and the time, manner and reason thereof can be identified;

13.2.5. Upon identification of a person and verification of person's identity data with IT means, the person's head and shoulders must be visible and framed. The face must be clear of shadows and uncovered, and clearly distinguishable from the background and other objects, and recognisable.

13.2.6. the person must have a possibility to change his or her body position and place themselves and the document in the frame to make it possible to identify the person and verify person´s identity, including viewing the data or images on the document.

13.3. The obliged entity has the right to require the change of body position and the removal of items covering the head or face and glasses or compliance with any other instructions of the obliged entity given in order to guarantee the identification of a person and verification of person's identity data.

13.4. The obliged entity must publish information about the technical conditions for the identification of a person and verification of person's identity with information technology means on its website or in the specified information system. At least the following facts must be presented in the published information:

13.4.1. a reference to the applicable legislative provisions;

13.4.2. the information that the identification of a person and verification of person's identity with information technology means take place according to the procedure set out in section 31 of the RahaPTS;

13.4.3. a warning that the identification of a person and verification of person's identity does not oblige the service provider to establish a business relationship or guarantee the accessibility of services;

13.4.4. the conditions in the event of which the identification of a person and verification of person's identity with information technology means is considered unsuccessful.

13.5. Before the identification of a person and verification of person's identity with IT means, the obliged entity is obligated to notify the person of the provisions set out in clause 13.4. and to receive confirmation that the person has received the notification. Additionally, the person to be identified is obligated to agree to the conditions of the identification of a person and verification of person's identity, by confirming the following;

13.5.1. the person carries out the procedure personally, except for the cases where the participation of third persons is necessary to solve technical problems;

13.5.2. the data submitted by him or her during the interview specified in clause 13.14 is correct and complete and he or she is aware of the consequences associated with the submission of incorrect, misleading or incomplete information upon the establishment of a business relationship;

13.5.3. he or she meets the conditions established by the service provider for the establishment of business relationships and the conclusion of transactions on occasional basis

13.6. In addition to the obligations set out in section 13.5., a natural person or legal representative of a legal entity who uses the e-resident's digital identity card or other high-reliability e-identification system must also:

13.6.1. agree with the application of Estonian law;

13.6.2. show to the obliged entity in front of the camera the personal data page of the valid travel document issued by the foreign country.

13.7. The identification of a person and verification of person's identity with the help of information technology means upon the establishment of a business relationship is considered unsuccessful if:

13.7.1. the natural person or the legal representative of a legal entity has intentionally submitted data that do not correspond to the identification data entered in the identity documents database or do not coincide with the information or data obtained with other procedures;

13.7.2. the session expires or is interrupted during the identification of a person, the identification questionnaire or the interview, or the information flow that transmits synchronised sound and image does not comply with the requirements set out in clause 13.2. The session expires when the natural person or the legal representative of the legal entity has not completed any activities in the service provider's information system during a period of 15 minutes;

13.7.3. the natural person or the legal representative of a legal entity has not given the confirmations prescribed in sections 13.4 and 13.5;

13.7.4. the natural person or the legal representative of a legal entity refuses to comply with the obliged entity's instructions specified in section 13.3;

13.7.5. the natural person or the legal representative of a legal entity uses the assistance of another person without the obliged entity's permission;

13.7.6. there are circumstances that give rise to suspicions of money laundering or terrorist financing.

13.8. In the event of circumstances prescribed in clauses 13.7.1 and 13.7.6, the obliged entity must send a notification thereof to the Financial Intelligence Unit.

13.9. The identification of a person and verification of person's identity with IT means takes place in the form of an identification questionnaire or an interview. On the basis of the collected data, the obliged entity prepares the customer profile of the person to be identified and the risk profile as a part thereof. The customer profile and the risk profile is prepared by the obliged entity in a form reproducible in writing.

13.10. The fulfilment of the preconditions of identification of a person and verification of person's identity data and the identification questionnaire are carried out by an employee of the obliged entity, a partner of the obliged entity or an automated system. The obliged entity is obligated to take measures in order to prevent the risks of the automated system being manipulated.

13.11. The identification questionnaire is used to ascertain the following:

13.11.1. In case of a natural person:

13.11.1.1. natural person's residential address;

13.11.1.2. activity profile;

13.11.1.3. area of activity;

13.11.1.4. purpose and nature of establishment of a business relationship;

13.11.1.5. connection of the person's economic or family interests with Estonia;

13.11.1.6. if appropriate:

13.11.1.6.1. expected volumes of the services used by the person;

13.11.1.6.2. the beneficial owner;

13.11.1.6.3. whether the person is a politically exposed person;

13.11.1.6.4. other important information.

13.11.2. In case of a legal entity:

13.11.2.1. legal entity's business name;

13.11.2.2. registry code;

13.11.2.3. location and places of operation;

13.11.2.4. including branches located in foreign countries;

13.11.2.5. entity's legal form;

13.11.2.6. legal capacity;

13.11.2.7. lawful and contractual representatives;

13.11.2.8. beneficial owner(s);

13.11.2.9. if appropriate:

13.11.2.9.1. whether the beneficial owner is a politically exposed person;

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

13.11.2.9.3. most important business partners;

13.11.2.9.4. the legal entity's activity profile;

13.11.2.9.5. main and secondary areas of activity;

13.11.2.9.6. purpose and nature of establishment of a business relationship;

13.11.2.9.7. other important information.

13.12. The employee of the obliged entity must assess the answers given in the identification questionnaire and record his or her opinion and the circumstances that are the basis thereof in the customer profile and risk profile specified in section 13.9.

13.13. The obliged entity may waive a separate identification questionnaire if the information specified in sections 13.1.1 and 13.11.2 is collected and the requirements specified in section 13.12 are complied with in the course of the interview.

13.14. In order to collect and verify the information and data required for the determination of the customer profile, the employee of the obliged entity carries out an interview, during which the employee asks partly structured questions, proceeding from the results of the identification questionnaire. If the interview is carried out with the questionnaire, at least the data specified in clause 13.11 must be acquired with the questions.

13.15. The employee of the obliged entity must carry on the interview that is mandatory for the establishment of a business relationship in real time. The employee of the obliged entity must assess the customer's reaction during the interview, the reliability of the obtained information and data and compliance with the information and data obtained with other procedures, and record his or her opinion and the circumstances that are the basis thereof in the customer profile and risk profile specified in section 11.9.

13.16. The information acquired during the questionnaire and the interview must be verified and preserved in accordance with the requirements set out for the application of due diligence measures and the procedures set out in the rules of procedure related to registration, verification and preservation of data.

14. IDENTIFICATION OF NATURAL PERSON AND REPRESENTATIVE

14.1. he obliged entity identifies the customer and, where relevant, their representative and retains the following data on the person and, where relevant, their representative:

14.1.1. first and last name;

14.1.2. personal identification code or, if none, the date and place of birth and the place of residence or seat;

14.1.3. information on the identification and verification of the right of representation and scope thereof and, where the right of representation does not arise from law, the name of the document serving as the basis for the right of representation, the date of issue, and the name of the issuer.

14.2. The employee makes a copy of the personal data and of the page including the photograph of the identity document for preservation, and the signature of the person making the copy along with the current date is attached to the copy. Where the identified person has a valid document specified in section 14.4 or an equivalent document, the person is identified and the person's identity is verified on the basis of the document or using means of electronic identification and trust services for electronic transactions, and the validity of the document appears from the document or can be identified using means of electronic identification and trust services for electronic transactions, no additional details on the document need to be retained.

14.3. The following valid documents specified in subsections 2(2) and 4(4) of the Identity Documents Act may be used as the basis for the identification of a natural person:

14.3.1. an identity card;

14.3.2. a digital identity card;
14.3.3. a residence permit card;
14.3.4. an Estonian citizen's passport;
14.3.5. a diplomatic passport;
14.3.6. a seafarer's discharge book;
14.3.7. an alien's passport;
14.3.8. a temporary travel document;
14.3.9. a travel document for a refugee;
14.3.10. a certificate of record of service on ships;
14.3.11. a certificate of return;
14.3.12. a permit of return;
14.3.13. a driving permit issued in the Republic of Estonia;
14.3.14. a driving permit issued in a foreign country if the document includes user's name, photograph or facial image, signature or image of a signature and date of birth or personal identification code;
14.3.15. a travel document issued in a foreign country.

14.4. Where the original document specified in section 14.4 is not available, the identity can be verified on the basis of a document specified in section 14.4, which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.

14.5. The obliged entity verifies the correctness of the data specified in subclauses 1-3 of clause 14.1, using information originating from a credible and independent source for that purpose.

14.6. During the verification of the data from a credible and independent source obtained during the identification of a natural person and representative, in accordance with clause 12.5,

14.6.1. one of the sources is always:

14.6.1.1. an identity document with a photo stipulated in clause 14.4 or a coloured and legible copy/image of this document; or

14.6.1.2. data and a photo of the person on the same document obtained from reliable and independent sources; or

14.6.1.3. the information (at least the name and personal identification code or the date and place of birth if there is no personal identification code) obtained in the course of strong authentication carried out with a digital personal identification tool if the money laundering and terrorist financing risk associated with the customer and the business relationship is lower than usual, and the audit trail proving that this was done.

14.6.2. The following information obtained from a reliable and independent source may be the second source:

14.6.2.1. another document that complies with the conditions in subclauses 1 or 2 of clause 14.6.1 (a copy thereof or the data and photo obtained therefrom); or

14.6.2.2. the information (at least the name and personal identification code or the date and place of birth if there is no personal identification code) obtained

in the course of strong authentication carried out with a digital personal identification tool and the audit trail proving that this was done; or

14.6.2.3. verification of the data directly related to a person via the Population Register or an equivalent register, provided that the source is a reliable and independent source within the meaning of clause 12.5 of these guidelines; or

14.6.2.4. information received from a first payment; or

14.6.2.5. other biometric data (fingerprint, facial image) or other information; or

14.6.2.6. information for checking the data directly associated with the person (e.g. place of work, residence or study).

14.7. In the case of representation, the obliged entity 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. The obliged entity must observe the conditions of the right of representation granted to the representatives and provide services only within the scope of the right of representation.

14.8. The representative of a foreign legal entity must submit, on the request of the obliged entity, 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.

14.9. When the right of representation of authorised and legal representatives is handled, it must be ascertained 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.

15. IDENTIFICATION OF LEGAL ENTITY

15.1. The obliged entity identifies the legal entity and retains the following data regarding the entity:

15.1.1. business name or name (with the legal form) of the legal entity;

15.1.2. registry code or registration number and date;

15.1.3. 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 these guidelines;

15.1.4. also the collection and retention of other data directly related to the entity, such as:

15.1.4.1. location of the legal entity, whereby the theory of the country of establishment must be proceeded from;
15.1.4.2. place of business of the legal entity;
15.1.4.3. data of the means of communication of the legal entity.
15.2. The following documents are used for identification of the legal entity:
15.2.1. registry card of the relevant register;
15.2.2. registration certificate of the relevant register; or
15.2.3. a document equivalent with an aforementioned document or relevant document of establishment of the legal entity.
15.3. The obliged entity verifies the correctness of the data specified in clause 15.1, using information originating from a credible and independent source for that purpose. Where the obliged entity has access to the commercial register, register of non-profit associations and foundations or the data of the relevant registers of a foreign country, the submission of the documents specified in section 15.2 does not need to be demanded from the customer.
15.4. Where the original document specified in section 15.2 is not available, the identity can be verified on the basis of a document specified in section 15.2, which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.
15.5. During the verification of the data from a credible and independent source obtained during the identification of a legal entity, in accordance with clause 12.5, the source shall be considered credible and independent when the obliged entity:
15.5.1. sees the original of the document specified in clause 15.2;
15.5.2. sees a copy of the document specified in clause 15.2 that has been authenticated by a notary, certified by a notary or officially certified; or
15.5.3. has access to the data in the commercial register, register of non-profit associations and foundations or the relevant registers of foreign countries via a computer network.
15.6. The documents specified in clause 15.2. must be issued by a competent authority or body not earlier than six months before their submission to the obliged entity.
15.7. In situations not specified in clause 15.5, the reliable and independent source is verification of the information obtained in the course of identification which originates from two different sources and complies with the requirements specified in clauses 12.5.1-12.5.3. Provisions of clause 15.5 must be applied in situations where the representative of a legal entity must be identified face-to-face according to clause 12.2.
15.8. Within the meaning of clause 12.5, two different sources during the identification of a legal entity means that the data medium, place or measure of obtaining information must be different (i.e. it cannot be the same data medium).
15.9. In addition to the document specified in clause 15.2 (if the obliged entity does not select two different identity documents of the customer 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.).

15.10. Public documents use to identify a legal entity issued in a foreign country must be legalised or confirmed with a certificate replacing legalisation (apostille) unless otherwise provided for in an international agreement.

15.11. In the case of documents in foreign languages, the obliged entity has the right to demand translation of the documents to a language they understand. The use of translations should be avoided in situations where the original documents are prepared in a language understandable to the obliged entity.

16. BENEFICIAL OWNER AND THEIR IDENTIFICATION

16.1. Upon the establishment of a business relationship or completing an occasional transaction, the obliged entity must identify the beneficial owner of the customer 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 obliged entity to make sure that they know who the beneficial owner is.

16.2. 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 in whose interests or for whose benefit or on whose account a transaction or act, action, operation or step is made. In the case of companies, a beneficial owner is the natural person who 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.

16.3. The obliged entity must understand the ownership and control structure of the customer or the person participating in an occasional transaction upon the establishment of a business relationship or the completion of an occasional transaction.

16.4. The beneficial owner does not have to be identified:

16.4.1. in the case of a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information;

16.4.2. in the case of an apartment association provided for in the Apartment Ownership and Apartment Associations Act;

16.4.3. in the case of a building association provided for in the Building Association Act.

16.5. The beneficial owner of a legal entity is identified in stages where the obliged entity 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:

16.5.1. is it possible to identify, in respect of the customer 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;

16.5.2. whether the customer that is a legal entity or the person participating in the transaction has a natural person or persons who own or control the legal entity

via direct or indirect shareholding. Family connections and contractual connections must also be taken into account here;

16.5.3. 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 obliged entity to identify the beneficial owner.

16.6. Direct ownership is a manner of exercising control whereby the natural person owns a 25 percent shareholding plus one share or an ownership right of over 25 percent in the company. Indirect ownership is a manner of exercising control whereby a 25 percent shareholding plus one share or an ownership right of over 25 percent in the company is owned by a company that is controlled by a natural person or several companies that are controlled by the same natural person.

16.7. A member of senior management specified in clause 16.5.3 is a person who:

16.7.1. makes the strategic decisions that fundamentally affect business activities and/or practices and/or the company general (business) trends; or in its absence

16.7.2. 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.).

16.8. Where, after all possible means of identification have been exhausted, the person specified in section 16.2 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, the natural person who holds the position of a senior managing official is deemed as a beneficial owner.

16.9. The obliged entity may consider beneficial owner to be a person who in some other way exercises control over the company without owning a 25 percent shareholding in that company. This situation also arises when the obliged entity suspects that some third person exercises significant control over the company whose ties to the company can not be legally proven or this proof is difficult to obtain. In such a situation, information must be demanded about the shareholders, partners and other persons who exercise control or other significant influence over the activities of the legal entity.

16.10. In the case of a trust, civil law partnership, community or another association of persons that does not have the status of a legal entity, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and who is the association's:

16.10.1. settlor or person who has handed over property to the asset pool;

16.10.2. trustee, asset manager or possessor;

16.10.3. person ensuring and controlling the preservation of assets, 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.

16.11. In the case of a company whose securities are traded on a regulated securities market, it is not necessary to identify the beneficial owners of such a company.

16.12. The obliged entity takes measures to verify the identified beneficial owner and does the same to an extent that makes it possible for the obliged entity to conclude that they know who the beneficial owner is. In the case of legal entities, this requires, in the case of identifying the purpose and nature of the business relationship, making it possible to conclude that the customer'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 that the obliged entity:

16.12.1. sees the original of the document specified in clause 15.2;

16.12.2. has access to the data in the commercial register, register of non-profit associations and foundations or the relevant registers of foreign countries via a computer network and checks the beneficial owner's data in said register;

16.12.3. sees a copy of the document specified in clause 15.2 that has been certified by a notary or officially certified;

16.12.4. uses other publicly accessible and/or reliable sources that are sufficient to make it possible to conclude who the beneficial owner is.

16.13. 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 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. Reasonable measures must be taken to verify the accuracy of the information established on the basis of statements or a handwritten document (e.g. by making inquiries in the relevant registers), requiring the submission of the legal entity's annual report or other relevant document.

16.14. If the obliged entity has doubts about the accuracy or completeness of the relevant information, the obliged entity shall verify the information provided from publicly available sources and, if necessary, request additional information from the person.

16.15. When determining the beneficial owner, particular attention must be paid to companies established in low-tax areas whose legal capacity is not always clear.

16.16. In the case of a trust, civil law partnership, community or other similar legal entity, assertation must be obtained about the nature of the beneficial owner on the basis of the civil law partnership agreement, letter of wishes, trust deed and other documents in addition to publicly accessible and/or reliable data. The provisions of clause 16.14 must be applied if the obliged entity wants to use the statement or handwritten document of the beneficial owner.

16.17. If another legal person has control over a legal person in accordance with the definition of beneficial owner, the obliged entity must assess the risk of the person or customer and collect data on other legal persons related to other persons to identify the beneficial owner.

16.18. The obliged entity is not required to independently inspect the ownership and control structure of a customer or a person concluding an occasional transaction and may rely on the statements or written explanations of the representative of the legal entity or trust, civil law partnership, community or other similar legal entity. This does not apply if the obliged entity has information that casts doubt on said circumstance, incl. it is in contradiction of the data obtained in the course of identification of the beneficial owner and the verification of data.

16.19. Upon the identification of a natural person, the obliged entity 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 obliged entity feels 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.

16.20. If the obliged entity ascertains that transactions or actions are actually performed on behalf of a third party, and the content of the activities suggests the possible activities of a trust, the obliged entity must take all measures to identify the beneficial owner of the trust and perform all actions to ascertain the actual purpose of the business relationship. For the purposes of the General Part of the Civil Code Act, this may mean that a business relationship with such a trust cannot be established, as the person who actually wants to establish the business relationship or perform the act is a trust that does not have legal capacity pursuant to Estonian law.

16.21. The obliged entity shall record and retain information of all operations carried out to identify the beneficial owner.

16.22. The obliged entity is prepared, if necessary, to explain the selection of the measure applied to the identification of the beneficial owner and the ownership and control structure and the verification measure selected for this purpose to Finantsinspektsioon.

17. POLITICALLY EXPOSED PERSON AND THEIR IDENTIFICATION

17.1. Upon the establishment of a business relationship and as in the course of a business relationship or if a certain trigger event occurs, the obliged entity will take measures to ascertain whether the customer or the person who wants to conclude an occasional transaction and the beneficial owner or representative of these persons is a politically exposed person (incl. high-risk politically exposed person), their family member or close associate, or if the customer has become such a person.

17.2. 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 chargé d'affaires and a highranking 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 obliged entity has the right to decide to update politically exposed official positions as a result of a risk-based approach and thereby also take additional measures in respect of other official positions.

17.3. In the case of a customer 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. In the case of a state-owned customer that is a legal entity or a person concluding an occasional transaction, the person must be considered a politically exposed person if the politically exposed person has a significant and prominent function in the company and the state owns at least 50% of this company. Upon the assessment of such a significant and

prominent function, it is necessary to also assess whether the politically exposed person has any (substantial) authorisation over the state's assets or funds or policies or activities, whether they have the right to issue licences or permits, make exceptions, whether they have control or influence over the accounts or funds of the state or the company, etc.

17.4. Local politically exposed person means a person specified in clause 17.2, who is or who has been entrusted with prominent public functions in Estonia, in another contracting state of the European Economic Area, or in a European Union institution.

17.5. 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.

17.6. A person known to be close associate means a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person or a local politically exposed person; 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 or local politically exposed person;

17.7. Obliged entities must identify close associates and family members of politically exposed persons only if their connection with the executor of substantial functions of public authority is known to the public or if the obliged entity has reason to believe that such a connection exists.

17.8. Where a politically exposed person no longer performs important public functions placed upon them, the obliged entity 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.

17.9. The obliged entity does not need to apply the due diligence measures provided for in this section with regard to a local politically exposed person, their family member or a person known to be their close associate where there are no other factors that refer to a higher-than-usual risk.

17.10. In addition to the relevant due diligence measures, the obliged entity applies inter alia the following additional measures to politically exposed persons:

17.10.1. requesting necessary information from the customer, including applying measures to establish the sources of the wealth and financial means of the person that are used in the business relationship or upon executing transactions;

17.10.2. verifying data or making inquiries in relevant databases or public databases or making inquiries or verifying data on the websites of the relevant supervisory authorities or institutions of the country in which the customer or person is located. The data is primarily verified as follows:

17.10.2.1. local politically exposed persons can be verified on the website of the Financial Intelligence Unit https://www.politsei.ee/et/organisatsioon/rahapesu/kasulikku/;

17.10.2.2. politically exposed persons of foreign countries can be verified by using the database NameScan https://namescan.io/FreePEPCheck.aspx, which is open-

access, and if possible, by using any paid databases (e.g., Thomson Reuters, MemberCheck, etc.);

17.10.2.3. both local and foreign politically exposed persons must be additionally verified using Google and the local search engine of the customer's country of origin, if any, by entering the customer's name in both Latin and local alphabet with the customer's date of birth.

17.11. In addition to the general due diligence measures specified in clause 17.10, the obliged entity applies the following measures to high-risk politically exposed persons:

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

17.11.2. 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;

17.11.3. monitors the business relationship in an enhanced manner as specified in these guidelines.

17.12. Senior management within the meaning of clause 17.11.1 is the person who has a sufficiently high position, the right to make decisions and thorough knowledge of the organisation and its capacity in order to make informed decisions in issues directly affecting the company's risk profile and who knows that the compensation mechanisms of the obliged entity are adequate for taking such risk.

18. IDENTIFICATION OF SOURCE AND/OR ORIGIN OF WEALTH

18.1. The obliged entity collects information about the source and/or origin of the customer's wealth:

18.1.1. upon the establishment of a business relationship, if appropriate, to identify the purpose and nature of the business relationship;

18.1.2. upon the conclusion of an occasional transaction outside of a business relationship, if appropriate, to identify the purpose and nature of the business relationship;

18.1.3. the obliged entity knows or suspects that the customer or the person concluding an occasional transaction is a high-risk politically exposed person, their family member or close associate.

18.2. Establishment of the source and/or origin of wealth means that the obliged entity identifies a bigger and more general picture of the customer's wealth, i.e. the source of all assets. This usually indicates how many funds the customer may have at all and where the customer received these funds from. In addition to requesting the relevant information from the customer, it may also be possible to collect such information from public databases and other public or non-public data, such as the land register, registers of other assets, declarations of economic interests, registers of companies, etc. 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 customer is particularly high. The obliged entity should not settle for the general answers of the customer or make unjustified assumptions (e.g. that employees with significant functions have bigger salaries and more assets etc.) and the obliged entity must be convinced that they know the source and/or origin of the

customer'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 non-publicly 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.

19. IDENTIFICATION OF PURPOSE AND NATURE OF BUSINESS RELATIONSHIP OR TRANSACTION

19.1. In the case of the establishment of a business relationship or an occasional transaction, the obliged entity must understand the purpose and nature of the business relationship or transaction.

19.2. In the appropriate case, the obliged entity must take additional measures and collect additional information to identify the purpose and nature. Such an appropriate situation occurs primarily in the cases where:

19.2.1. there is a situation that refers to high value or is unusual and/or

19.2.2. where the risk and/or risk profile associated with the customer 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.

19.3. The obliged entity makes sure that the service provided complies with the content of the customer's actual declarations of intent (why they want the service), complies with the nature and purposes of the specific contract and corresponds to the risk level assigned to the customer. The obliged entity must assess on the basis of the aforementioned information what the expected activities of the customer are like, i.e. on the basis of this information it will be possible for the obliged entity to later assess the activities of the customer 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).

19.4. The additional measure specified clause 19.1 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 customer or the person participating in an occasional transaction. The above is not an exhaustive list and, if necessary, the obliged entity 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 on-site visits before the establishment of the business relationship and applies other necessary measures.

19.5. In order to identify the **area of activity**, the obliged entity must understand what the customer 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.

19.5.1. The accuracy of the area of activity defined by the customer must correspond to the risk profile of the customer and the business relationship and the customer's risk level. For example, in the case of a risk that is higher than usual, this may not be economically unreasonably too broad or economically unreasonably

completely different from each other, which is why the area of activity allows the customer to basically deal with everything and does not allow the obliged entity to correctly monitor the business relationship.

19.5.2. Upon the identification of the area of activity, the obliged entity must also identify whether an authorisation for provision of a financial service is required for the service to be provided and whether the service is actually provided via the obliged entity to the customer's customers, i.e. to the ultimate beneficial owners to whom the obliged entity should apply due diligence measures.

19.6. In the case of **payment practices**, it is important to identify the manner in which financial services are consumed (for example, in the case of bank account, the approximate number, volume, purpose and frequency of transactions concluded per month and per year, the countries from which payments are received and to which payments are made, the expected duration of the business relationship, the extent and channels of cash use, payment channels (branch, Internet bank, card payments), etc.; (ii) the frequency, size and time of repayments related to the loan taken within the scope of the business relationship to be established; (iii) in the case of investment products, the recommended securities, the approximate quantities in which they will be purchased and the frequency of purchases, the information related to their realisation, the quantity of assets to be invested, the expected duration of the business relationship (one-off activity or similar), etc.).

19.6.1. The obliged entity must thereby identify whether, why and on which conditions the customer is capable of concluding such transactions at all and how this corresponds to the customer's knowledge in other respects and the risk profile of the customer and the business relationship in general. The performance of this obligation often calls for the more general identification of the source and/or origin of the customer's wealth.

19.7. In the case of **main business partners**, the obliged entity must identify who are the customer's main partners with whom transactions will be concluded in the declared area of activity and with the declared activity volumes, i.e. who the persons to realise the purpose of the establishment of the business relationship are.

19.7.1. The main business partners means the persons who make the conclusion of incoming and outgoing transactions possible, i.e. the main business partners must be identified in two separate categories.

19.7.2. The obliged entity must in the appropriate case, but primarily in the case of a risk that is higher than usual, also ascertain how these main business partners are associated with the area of activity, i.e. whether the information that also confirms activities in said area of activity is publicly accessible. The obliged entity must also ascertain in the appropriate case why these main business partners agree or are prepared (incl. on which preconditions) to conduct business with the customer, and this obligation primarily lies in the situation where the customer is a newly established company or a so-called shell company that was previously established, but starts conducting business at the specific moment in time.

19.7.3. If the service provided by the customer is purchase or sale of goods, asking about main business partners covers in the appropriate case, but primarily in the case of a risk that is higher than usual, asking about service providers that transport goods.

19.7.4. It is important in the appropriate case, but primarily in the case of a risk that is higher than usual, to also give attention to the locations of these main business partners and make sure that this coincides with the payment practices previously declared by the customer (especially in terms of countries from which funds are received and to which funds are transferred).

19.7.5. The obliged entity must make sure upon the establishment of the business relationship that transactions will really be concluded with the main business partners. The obliged entity will check this circumstance later in the course of the business relationship.

19.8. The area of activity specified in clauses 19.4-19.6, payment practices and main business partners must thereby fit into the experience profile of the customer's representative (or key persons) and/or the beneficial owner. Thus the obliged entity has to identify where the representative's and/or beneficial owner's capacity, capability, skills and knowledge (experience in general) comes from in order to operate in this area of activity, with these business volumes and with these main business partners.

19.8.1. The identification of experience is often not limited to just requesting CVs, but requires a substantive understanding and analysis of how the customer's previous knowledge fits into the customer's business activity. Consequently, it has to be established whether the business relationship or transactions are in compliance with the customer's ordinary participation in commerce and whether the business relationship or transaction has a clear economic reason.

20. PERSON OPERATING IN HIGH-RISK THIRD COUNTRY

20.1. High-risk third country means a country specified in a delegated act adopted on the basis of Article 9(2) of Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141/73, 05.06.2015, pp 73–117).

20.2. High-risk third countries include Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, Lao PDR, Syria, Uganda, Vanuatu, Yemen, Iran, DPR Korea;

20.3. Where the obliged entity 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 a professional act, via a person using a professional service or via a customer, the obliged entity applies the following due diligence measures:

20.3.1. gathering additional information about the customer and its beneficial owner;

20.3.2. gathering additional information on the planned substance of the business relationship;

20.3.3. gathering information on the origin of the funds and wealth of the customer and its beneficial owner;

20.3.4. gathering information on the underlying reasons of planned or executed transactions;

20.3.5. receiving permission from the senior management to establish or continue a business relationship;

20.3.6. 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.

20.4. In addition to the aforementioned, the obliged entity 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.

21. DUE DILIGENCE MEASURES DURING BUSINESS RELATIONSHIP

21.1. The obliged entity must observe the business relationship with the customer established in the course of economic or professional, i.e. perform the monitoring of the business relationship.

21.2. The obliged entity shall implement the following measures as part of the monitoring of the business relationship:

21.2.1. ensuring 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;

21.2.2. continuous monitoring of the business relationship, which covers transactions carried out in the business relationship to ensure that the transactions correspond to the obliged entity's knowledge of the customer, their activities and risk profile;

21.2.3. identification of the source and origin of funds used in a transaction.

21.3. The obliged entity must regularly check and update the documents, data and information collected in the course of the application of due diligence measures. The regularity of the checks must be based on the risk profile of the customer and the checks must take place at least:

21.3.1. once semi-annually for a high-risk profile customer;

21.3.2. once annually for a medium-risk profile customer;

21.3.3. once every two years for a low-risk profile customer.

21.3.4. The collected documents, data and information must also be checked if an event has occurred which indicates the need to update the collected documents, data and information.

21.4. In the course of the **ongoing monitoring of a business relationship**, the obliged entity must monitor the transactions concluded during the business relationship in such a manner that the latter can determine whether the transactions to be concluded correspond to the information previously known about the customer (i.e. what the customer declared upon the establishment of the business relationship or what has become known in the course of the business relationship). The obliged entity must also monitor the business relationship to ascertain the customer'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, high-value 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. In the course of the business relationship, the obliged entity must constantly assess the changes in the customer's activities and assess whether these changes may increase the risk level associated with the customer and the business relationship, giving rise to the need to apply additional or enhanced due diligence measures.

21.5. In the course of the ongoing monitoring of the business relationship, the obliged entity applies the following measures:

21.5.1. screening i.e. monitoring transactions in real-time;

21.5.2. monitoring i.e. analysing transactions later;

21.6. The objective of **screening** is to identify:

21.6.1. suspicious and unusual transactions and transaction patterns;

21.6.2. transactions exceeding the provided thresholds;

21.6.3. politically exposed persons and circumstances regarding international sanctions.

21.7. The measures taken for screening must be risk-based, i.e. comply with the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and risks arising from activities of the obliged entity.

21.8. If obliged entities use automatic systems to identify suspicious and unusual transactions carried out within the scope of specific business relationships, they should ensure that these systems are expedient, i.e. they should be consistent with the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and risks arising from activities of the obliged entity. The parameters/scenarios of the automatic system must:

21.8.1. really cover the risks and threats the obliged entity primarily faces in their activities in order to identify suspicious and unusual transactions (and transactions patterns, if possible);

21.8.2. make it possible to identify transactions (incl. card transactions, if possible) that are made, transferred or received from countries or, if possible, from the neighbouring countries of these countries, which are associated with a higher risk of terrorism, incl. are areas of conflict, or from countries that have other important connections with the aforementioned countries;

21.8.3. also cover the descriptions of transactions and the information therein;

21.8.4. in order to identify a subject of international sanctions, cover the capability to verify the compliance of data in respect of the customer, their representative and the beneficial owner;

21.8.5. in order to identify politically exposed persons, cover the capability to verify the compliance of data in respect of the customer, their representative and the beneficial owner;

21.8.6. guarantee the identification of persons (covers the person themselves, their representative and beneficial owner) in respect of whom the obliged entity has had prior suspicions or with whom they have refused to establish a business relationship or whose business relationship has been extraordinarily terminated (incl. in the case this is technically possible and not too burdening for the obliged entity, inspection of the IP addresses used by these persons). The objective of this is to allow the obliged entity to take measures if the same persons want to establish a business relationship again;

21.8.7. ensure that the obliged entity can identify concealed or obvious (business) ties between different customers (belonging to the same group) of which the obliged entity was previously not aware.

21.9. Upon the selection of an automatic IT system, the obliged entity must ensure that such monitoring takes place at least once a week, excl. subclauses 1-3 of clause 19.8, which has to take place in real time, also excl. subclause 4, which must also take place in real time if the obliged entity does not take measures every time when changes are made in international financial sanctions.

21.10. If the obliged entity does not select an appropriate IT system, their manual monitoring systems must cover the principles stipulated in clause 19.8.

21.11. The objective of **monitoring** is 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 customer types).

21.12. Monitoring may take place with the help of parameters determined by the obliged entity, the sample list of which is as follows:

21.12.1. (private and corporate) accounts with larger turnovers in the period under review, borrowers, users of investment services, buyers of funds units, etc. by currencies (of natural persons and legal entities);

21.12.2. larger transactions (of private and corporate customers) in the period under review by currency (of natural persons and legal entities) and service;

21.12.3. transactions via ATMs carried out in the period under review that exceed a certain threshold;

21.12.4. cash withdrawals and deposits at branches and ATMs that exceed a certain threshold (by natural persons and legal entities);

21.12.5. unexpected increase in the turnover of VOSTRO accounts in correspondent relationships;

21.12.6. transactions of a certain customer (type).

21.12.7. number of accounts the customer uses to carry out transactions;

21.12.8. number of high-risk customers and their connections between each other;

21.13. The obliged entity must pay enhanced attention i.e. apply enhanced due diligence measures to transactions and transaction patterns that are complicated, high-value 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.

21.14. In addition to the application of enhanced due diligence measures, the background of each single transaction specified in clause 19.12 must be investigated to the extent that is reasonably necessary, incl. the details of the transaction must be specified and any circumstances that have emerged must be analysed in order to identify the most typical features of the most frequent transactions. These data must be retained. The main circumstances to which attention must be given in analysing such transactions are as follows:

21.14.1. the circumstance by the acts, transactions or other circumstances that caused suspicion;

21.14.2. whether the obliged entity is convinced that they know the customer to the necessary extent and whether the customer's activity correspond to the

information previously known about the customer or whether additional data need to be collected about them and whether reasonable and adequate measures need to be taken to understand the background and purpose of the transaction, e.g. by identifying the source and destination of the funds or looking for more information about the customer's activities in order to identify that such a transaction is true;

21.14.3. whether there have been repeated signs of suspicious acts and transactions (incl. in respect of similar situations or circumstances);

21.14.4. whether it is necessary to give more attention to the customer's activity and the business relationship in general in the future, incl. to details;

21.14.5. whether the obligation to report to the Financial Intelligence Unit must be performed.

21.15. The representative of the obliged entity may perform on-site visits to the customer as part of monitoring to verify whether the customer's explanations of their capability and capacity are true.

21.16. In the course of the business relationship, the obliged entity identifies the **source and origin of the funds used in a transaction** if necessary. 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 clause 21.2 and the objective provided therein, with the difference being that whilst the monitoring of the business relationship covers the entire business relationship of the customer 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 customer and find out whether this corresponds to the information previously known about the customer. This is why all of the explanations under the general principles of clause 21.4 apply to the source and origin of the funds used in the transaction.

21.16.1. The source of the funds used in the transaction is reason, explanation and basis (legal relationship and its content) why the funds were transferred.

21.16.2. The origin of the funds used in the transaction is the activity by which the funds were earned or received and is closer to the identification of the source and/or origin of wealth (see section 18).

21.17. 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 customer's previous activities as well as other known information. Thereby the need for identification of the source and origin of the funds increases:

21.17.1. proportionally to the size of the funds;

21.17.2. if the transactions do not correspond to the information previously known about the customer;

21.17.3. if the obliged entity wants to or should reasonably consider it necessary to assess whether the transactions correspond to the information previously known about the customer;

21.17.4. 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, high-value 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.

21.18. The origin is broader and includes the activity with which the funds were earned or received and is closer to the identification of the source and/or origin of wealth (see also section 18).

22. OUTSOURCING ACTIVITY TO ANOTHER PERSON

22.1. The obliged entity has the right, considering the special requirements and restrictions stipulated in legislation, to use the services of another person on the basis of a contract, the content of which is the continued performance of activities and acts that are necessary for the provision of the service(s) by obliged entities to customers and that would ordinarily be performed by the obliged entity themselves. Another person within the meaning of this point is, for example, an agent, subcontractor or another person to whom the obliged entity outsources an activity related to the provision of these services, which the obliged entity performs themselves in their economic activities as a rule. The obliged entity outsources an activity in a situation where another person implements the requirements arising from the RahaPTS and/or these guidelines on behalf and for the account of the obliged entity. This obligation differs from relying on another person where the other person implements the requirements arising from the RahaPTS and/or these guidelines 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.

22.2. In order to outsource an activity within the meaning of clause 22.1, the obliged entity must implement an outsourcing policy/risk assessment that is approved by the management board of the obliged entity. At least the following must be analysed, considered and described in this document:

22.2.1. the impact of outsourcing on the business activities of the obliged entity and the manifesting risks (e.g. operational risk, incl. IT and legal risk, reputation risk and concentration risk);

22.2.2. the reporting and supervision procedure implemented from the start to the end of the outsourcing contract (incl. preparation of the description of outsourcing, entry into the outsourcing contract, performance of the contract until its expiry, situation plans and strategies for termination of the contract);

22.2.3. in the event of outsourcing an internal activity of the consolidation group, the procedure for outsourcing, incl. the services provided by a legal entity belonging to the consolidation group of the obliged entity, and the specific features of the consolidation group;

22.2.4. the procedure and methodology for selecting and assessing the other person.

22.3. The obliged entity may outsource the obligation to fully or partly apply the due diligence measures specified in sections 11 to 20 (i.e. the identification of the customer, beneficial owner, politically exposed person, the source and/or origin of wealth and the purpose and nature of the business relationship) only:

22.3.1. to another obliged entity;

22.3.2. to an organisation, association or union whose members are obliged entities; or

22.3.3. to another person who applies the due diligence measures and data retention requirements provided for in the RahaPTS and in these guidelines and who is subject to or is prepared to be subject to AML supervision or financial supervision in a contracting state of the European Economic Area regarding compliance with requirements.

22.4. The obligation to apply due diligence measures not specified in clause 22.3 cannot be outsourced. This restriction does not apply to outsourcing activities related to the identification and implementation of international sanctions.

22.5. The obliged entity selects the other person specified in clause 22.1 with due diligence to ensure the capacity of this person to comply with the requirements of the RahaPTS and these guidelines and ensure the reliability and necessary qualification of this person. When outsourcing the activity (activities) of the obliged entity, the obliged entity must ensure that the other person has the required knowledge and skills, primarily for identifying suspicious and unusual situations, and that they are capable of complying with all of the money laundering and terrorist financing prevention requirements stipulated by legislation. In order to comply with the provisions of this clause, the obliged entity must make sure that the managers of the other entity are informed about the relevant requirements and ensure training of employees about the prevention of money laundering and terrorist financing to a necessary extent.

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

22.6.1. division of the rights and obligations associated with the outsourcing of the activity, incl. data retention, reporting to the Financial Intelligence Unit(s), etc.;

22.6.2. that the outsourcing of the activity does not impede the activities of the obliged entity or performance of the obligations provided for in the RahaPTS and these guidelines;

22.6.3. that the other person performs all the obligations of the obliged entity relating to the outsourcing of the activity;

22.6.4. that the outsourcing of the activity does not impede exercising supervision over the obliged entity;

22.6.5. that the competent authority can exercise supervision over the person carrying out the outsourced activity via the obliged entity, incl. by way of an on-site inspection or another supervisory measure;

22.6.6. the required level of knowledge and skills and the capacity of the other person and the set of measures taken for this purpose, incl. regular training;

22.6.7. that the obliged entity has the unrestricted right to inspect compliance with the requirements provided for in the RahaPTS and these guidelines;

22.6.8. that documents and data gathered for compliance with the requirements arising from the RahaPTS and these guidelines are retained and, at the request of the obliged entity, copies of documents relating to the identification of a customer and their beneficial owner or copies of other relevant documents are handed over or submitted to the competent authority immediately. The contract must guarantee that any information that is relevant in the course of the application of due diligence measures is handed over to the obliged entity and/or the relevant data and documents are archived pursuant to the procedure set forth in their rules of procedure;

22.6.9. the right of the obliged entity to terminate the outsourcing contract with the other person, where necessary, if the latter has failed to perform the contractual obligations or has not performed them properly.

22.7. The obliged entity immediately informs the competent supervisory authority about entry into the contract that serves as a basis for outsourcing their activity (activities). When providing information, the obliged entity shall indicate, inter alia, the scope of the transferred activity. At the request of the competent supervisory authority, the obliged entity shall provide the contract for the outsourcing of activities.

22.8. The obliged entity is not allowed to outsource activities to an entity that has been established in a high-risk third country.

22.9. All of the money laundering and terrorist financing prevention requirements stipulated by legislation extend to the other person in respect of the outsourced activity (activities) within the meaning of clause 20.1. The obliged entity that has outsourced an activity is responsible for compliance with requirements and therefore also for any violations.

23. RELYING ON THIRD PARTY

23.1. The obliged entity relies on a third party in a situation where a third party implements the requirements arising from the RahaPTS and/or these guidelines 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 RahaPTS and/or these guidelines on behalf and for the account of the obliged entity.

23.2. The obliged entity may rely on the data and documents gathered by another person upon the partial or full application of the due diligence measures specified sections 11 to 17 (i.e. the identification of the customer, beneficial owner and politically exposed person) if the obliged entity:

23.2.1. 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;

23.2.2. 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;

23.2.3. 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.

23.3. The obliged entity takes adequate measures to ensure performance of the obligations stipulated in clause 23.2, incl. enters into a contract for this purpose if necessary and applies other measures.

23.4. The obliged entity is not allowed to rely on an entity that has been established in a high-risk third country.

23.5. The obliged entity that relies on the third party is responsible for compliance with requirements and therefore also for any violations.

24. REFUSAL TO ESTABLISH BUSINESS RELATIONSHIPS AND CARRY OUT TRANSACTIONS

24.1. The obliged entity **is prohibited to establish a business relationship or allow to execute an occasional transaction** or conclude it if:

24.1.1. the obliged entity suspects money laundering or terrorist financing or it is impossible for the obliged entity to apply the due diligence measures taken upon the establishment of business relationships, because the customer 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;

24.1.2. a person whose capital consists of bearer shares or other bearer securities wants to establish a business relationship or conclude an occasional transaction;

24.1.3. 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;

24.1.4. this would require the opening of an anonymous account or savings book, as well as the opening of an account clearly in the name of the wrong person;

24.1.5. a natural person behind whom is another, actually benefiting person, wants to establish a business relationship or conclude an occasional transaction (suspicion that a person acting as a front is used).

24.2. The obligation arising from clause 24.1 must not be performed if the obliged entity has informed the Financial Intelligence Unit about the establishment of the business relationship, an occasional transaction or an attempt to conclude a transaction pursuant to the procedure stipulated in section 26 and/or received a specific instruction from the Financial Intelligence Unit to continue establishing the specific business relationship or concluding the occasional transaction.

24.3. In respect of the circumstances of refusal to establish a business relationship or conclude an occasional transaction, the obliged entity performs the reporting obligation according to the requirements set out in section 26 and registers and retains the data of the refusal to establish a business relationship or conclude an occasional transaction as well as of the performance of the reporting obligation according to the requirements set out in section 27.

24.4. In a situation where the obliged entity constantly refuses to establish a business relationship or conclude an occasional transaction on the basis of clause 24.1 or if the above is refused before the application of due diligence measures, the obliged entity must carry out periodical analyses to identify:

24.4.1. who the employees or other contractual partners are who primarily bring in the customers with whom the obliged entity refuses to establish a business relationship or conclude an occasional transaction;

24.4.2. who the agency, representation or other person is who brings in the customers with whom the obliged entity refuses to establish a business relationship or conclude an occasional transaction.

24.5. The obliged entity has **the right to refuse to make a transaction within the scope of a business relationship** where a person participating in a transaction or a customer, 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 obliged entity suspect money laundering or terrorist financing or the commission of related crimes or an attempt at such activity.

24.6. If the data are insufficient or untrue or if there are suspicions of money laundering or terrorist financing, the obliged entity 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.

24.7. If the obliged entity has still not managed to apply adequate due diligence measures within reasonable time in order to exhaustively collect data, make sure that the data are true or eliminate suspicions of money laundering or terrorist financing, the obliged entity must terminate the business relationship extraordinarily according to the requirements set forth in clause 24.10.

24.8. The obliged entity **has the right to terminate the long-term contract serving as a basis for a business relationship extraordinarily and without notice** if:

24.8.1. a person is not issued an e-resident's digital identity card, its validity is suspended or it is declared invalid on the ground stipulated in subsections 20^6 (2) or (3) of the Identity Documents Act;

24.8.2. a person is suspected of money laundering, excl. the situation stipulated in clause 24.7.

24.9. The obliged entity **is required to terminate the long-term contract that serves as a basis for the business relationship extraordinarily without notice** if the business relationship has been established and the due diligence measures cannot be applied again, because the circumstance specified in clause 24.7 are present or because the customer 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.

24.10. In the event of an extraordinary termination of a business relationship within the meaning of clauses 24.8 and 24.9, the obliged entity will transfer the customer's assets within reasonable time, but preferably not later than within one month after the extraordinary termination of the business relationship and as a whole to an account opened in a credit institution entered in the Commercial Register in Estonia or in a branch of a foreign credit institution or a credit institution which is registered or whose place of business is in a contracting state of the European Economic Area or in a country where requirements equal to those established in the relevant directives of the European Parliament and of the Council are applied. In exceptional cases, assets may be transferred to an account other than the customer's account or issued in cash by informing the Financial Intelligence Unit about this with all the relevant and sufficient information at least 7 working days in advance and on the condition that the Financial Intelligence Unit does not give a different order. Irrespective of the recipient of the funds, the minimum information given in English

in the payment details of the transfer of the customer's assets is that the transfer is related to the extraordinary termination of the customer relationship.

24.11. In respect of the circumstances of mandatory extraordinary termination of a business relationship, the obliged entity performs the reporting obligation according to the requirements set out in section 26 and registers and retains the data of the extraordinary termination of the business relationship and the performance of the reporting obligation according to the requirements set out in section 27.

24.12. The right arising from clauses 24.5 and 24.8 must not be exercised and the obligation arising from clause 24.9 must not be performed if the obliged entity has informed the Financial Intelligence Unit about the establishment of the business relationship, the transaction or attempted transaction pursuant to the procedure stipulated in section 26 and received a specific instruction from the Financial Intelligence Unit to continue with the business relationship or the transaction. The right may also not be exercised if the obliged entity has received instructions from the Financial Intelligence Unit without the prior relevant report.

24.13. In a situation where the obliged entity constantly terminates business relationships extraordinarily on the basis of clause 24.9, the obliged entity must carry out periodical analyses to identify:

24.13.1. who the employees or other contractual partners are who primarily bring in the customers with whom business relationships are extraordinarily terminated and whether such persons have failed to perform their duties or have performed them inadequately;

24.13.2. who the agency, representation or other person is who brings in the customers with whom business relationships are extraordinarily terminated and whether such persons have failed to perform their duties or have performed them inadequately;

24.13.3. which employees manage the customers with whom business relationships are most often terminated and what the reason for this is as well as whether such persons have failed to perform their duties or have performed them inadequately;

24.13.4. whether it would have been possible to identify the bases for the extraordinary termination of a business relationship upon the establishment of the business relationship or at an earlier moment in the life cycle of the business relationship and why these circumstances were not identified then.

25. APPLYING INTERNATIONAL SANCTIONS

25.1. Upon the entry into force of an act establishing or implementing an international financial sanction, the obliged entity shall take measures to fulfill the obligations arising therefrom and shall show the necessary diligence to ensure the achievement of the objective of the international financial sanction and to prevent violation of the sanction.

25.2. The definition of international sanction:

25.2.1. International sanctions are an essential tool of foreign policy aimed at supporting the maintenance or restoration of peace, international security, democracy and the rule of law, following human rights and international law or achieving other

objectives of the United Nations Charter or the common foreign and security Policy of the European Union.

25.2.2. International sanctions are imposed with regard to a state, territory, territorial unit, regime, organisation, association, group or person by a resolution of the United Nations Security Council, a decision of the Council of the European Union or any other legislation imposing obligations on Estonia.

25.2.3. International sanctions may ban the entry of a subject of an international sanction in the state, restrict international trade and international transactions, and impose other prohibitions or obligations.

25.2.4. The sanctions of the Government of the Republic of Estonia is a tool of foreign policy which may be imposed in addition to the objectives specified in previous clauses in order to protect the security or interests of Estonia.

25.3. The subject of international sanctions is any natural or legal person, entity or body, designated in the legal act imposing or implementing international sanctions, with regard to which the international sanctions apply.

25.4. Within the meaning of these guidelines, financial sanctions are international sanctions which:

25.4.1. obligate the freezing of funds and economic resources of the subject of international financial sanctions;

25.4.2. prohibit the making available of financial and economic resources to the subject of the financial sanctions;

25.4.3. prohibit the granting of loans and credit under the conditions prescribed by the legislation on implementation of international sanctions;

25.4.4. prohibit the opening and use of a deposit, payment, securities or other account under the conditions prescribed by the legislation on implementation of international sanctions;

25.4.5. prohibit the securities transactions under the conditions provided for in the legislation on implementation of international sanctions;

25.4.6. prohibit the conclusion of an insurance contract under the conditions prescribed by the legislation on implementation of international sanctions;

25.4.7. prohibit investing under the conditions prescribed by the legislation on implementation of international sanctions; or

25.4.8. prohibit, under the conditions provided for by the legislation on implementation of international sanctions, the starting or continuing of business relationships, consultancy or the provision of other financial services related to the activities listed above.

25.5. A person having specific obligations is:

25.5.1. a credit institution within the meaning of the Money Laundering and Terrorist Financing Prevention Act;

25.5.2. a financial institution;

25.5.3. a person having the status of an account operator within the meaning of the Securities Register Maintenance Act and the Central Securities Depository if the person arranges for the opening of securities accounts and provides services related to registry operations without intermediation of an account operator;

25.5.4. a branch of a foreign service provider entered in the Estonian commercial register providing the same type of service as the agencies specified in clauses 25.5.1-25.5.3.

25.6. In economic or professional activities, the obliged entity shall pay special attention to such activities and circumstances of the person who has a business relationship, performs a transaction or an act with them, or who intends to establish a business relationship, perform a transaction or an act with them, which indicate that the person may be a subject of an international financial sanction.

25.7. Upon the entry into force, amendment or termination of financial sanctions, a person having specific obligations shall verify whether the person who has or is planning to have a business relationship with them is a subject of financial sanctions. If the person having specific obligations identifies a person who is a subject of financial sanctions or that the transaction or act intended or carried out by them is in breach of financial sanctions, the person having specific obligations shall apply financial sanctions and immediately inform the Financial Intelligence Unit thereof.

25.8. If a person having specific obligations has doubts whether a person who has or is planning to have a business relationship with them is a subject of financial sanctions or that a transaction or act which is planned or carried out by them violates financial sanctions, the person having specific obligations shall apply financial sanctions and the due diligence measures as follows:

25.8.1. collect additional information as to whether the person who has or intends to have the business relationship with them is a subject of financial sanctions or whether a transaction or act which is planned or carried out violates financial sanctions and verify it on the basis of supporting documents, data or information from a reliable and independent source;

25.8.2. collect additional information regarding the purpose and nature of the business relationship, transaction or act and verify it on the basis of additional documents, data or information from a reliable and independent source.

25.8.3. A person having specific obligations shall also apply the due diligence measures in the event of a risk or suspicion of a violation of a financial sanction.

25.8.4. If, as a result of application of due diligence measures, the person having specific obligations identifies a subject of the financial sanction or that the transaction or act which is planned or carried out by them violates financial sanctions, or if additional information obtained upon application of due diligence measures does not enable to identify it, as well as in the case of the suspicion of violation of financial sanction specified in section 25.8.3, the person having specific obligations shall inform the Financial Intelligence Unit thereof and of the financial sanction applied.

25.9. The obliged entity shall regularly visit the website of the Financial Intelligence Unit and shall immediately take the measures provided for in the legislation establishing or implementing international financial sanctions in order to ensure the achievement of the objective of the international financial sanctions and to prevent violation of the international financial sanctions.

25.10. Upon entry into force of an act establishing or implementing an international financial sanction, the employees of the obliged entity shall apply the necessary diligence to ensure the achievement of the objective of the international financial sanction and to prevent violation of the sanction.

25.11. The employees of the obliged entity shall apply additional diligence in establishing a business relationship and concluding transactions with regard to the customer and the circumstances of the transaction (incl. to the other party of the transaction).

25.12. The employees, management board and compliance officer of the obliged entity shall pay special attention during the economic activities of the obliged entity to such activities and circumstances of the person who has a business relationship, performs a transaction or an act with them, or who intends to establish a business relationship, perform a transaction or an act with them, which indicate that the person may be a subject of an international financial sanction.

25.13. Pursuant to the International Sanctions Act, the person having specific obligations have the obligation of applying additional due diligence measures to verify the events where international sanctions must be applied. For this purpose, the aforementioned persons must:

25.13.1. notify the Financial Intelligence Unit of the subject of the international sanction and the application of the financial sanction on the basis thereof;

25.13.2. in an event of a suspicion of subject of a financial sanction, to collect additional information and if the suspicion persists, notify the Financial Intelligence Unit;

25.13.3. notify the Financial Intelligence Unit of the refusal to establish a business relationship or to conclude a transaction if the basis of the refusal was based on the possible involvement of a person, country, transaction, or goods which the transaction is based on, in an international sanctions regime.

25.14. Procedure for identifying the subject of a financial sanction and a transaction or act violating the financial sanction:

25.14.1. The obliged entity verifies whether the person in a business relationship with them or intending to establish a business relationship is subject to international sanctions. The obliged entity also verifies whether the person with whom they are in a business relationship carries out transactions with the subjects of international sanctions.

25.14.2. In order to identify the persons specified in the legislation on international sanctions, the obliged entity's internal databases and databases managed by third parties shall be consulted in order to establish the existence of such persons or transactions with them.

25.14.3. To verify that the persons' names resulting from the inquiry are the same as the persons listed in a notification containing an international sanction, mostly their personal data is used, the main characteristics of which are, for a legal entity, its name or trademark, registry code or registration date, and for a natural person, their name and personal identification or date of birth.

25.14.4. Inquiries must be made primarily on the basis of the personal data provided in the relevant notice regarding the person who is the subject of the sanction. When preparing the inquiry, the factors distorting personal data must be taken into account when describing the parameters of the inquiry.

25.14.5. The factors distorting personal data include circumstances that may change the written representation of the personal data. Based on the manifestation of the factors distorting personal data, the data in databases (mainly the names of persons) may differ from the actual name of the person and/or the data (name) of the person in the notification containing an international sanction.

25.14.6. In order to establish the identity of the persons specified in the relevant legal act or notice being the same as those identified as a result of the inquiry from databases, the obliged entity must analyse the names of the persons found as a

result of the inquiry based on the possible effect of factors distorting personal data.

25.14.7. The factors distorting personal data include the following mistakes or differences emerging in the course of translation, handling or processing of the personal data and names:

25.14.7.1. transcribing foreign names, incl. the differences arising from the latinisation of Russian and Scandinavian names;

25.14.7.2. different order of words in the name composed of several words, e.g. AS JAAN TAMM or TAMM JAAN AS;

25.14.7.3. substitution of diacritics (letters with dots or emphasis) with other letters or their (partial) omission;

25.14.7.4. substitution of double letters and foreign letters other letters or their (partial) omission:

25.14.7.4.1. substitution of double letters with a single letter (and vice versa), e.g. METALL or METAL;

25.14.7.4.2. substitution of letters F, Š, Z, Ž, C ... with other letters or letter combinations, e.g. FARMA or PHARMA, CRISTAL or KRISTAL;

25.14.7.4.3. substitution of foreign letters W, Q, X, Y ... with other letters , e.g. WOX QYIT or VOKS KÜIT;

25.14.7.4.4. use of abbreviations;

25.14.7.4.5. typing numbers as words in a text, e.g. 2 FAST 4 YOU or TWO FAST FOUR/FOR/ YOU;

25.14.7.5. use/non-use of additional and preceding words (and letters, prefixes);

25.14.7.6. other factors:

25.14.7.6.1. arising from human error;

25.14.7.6.2. replacing hard and soft consonants, e.g. AS GAASI KÜTE or AS KAASI GÜTE;

25.14.7.6.3. the name or part of the name appearing before or as part of the other name.

25.14.8. If the person having specific obligations is not able to unambiguously identify the persons as the result of the inquiry, taking into account the factors distorting personal data, being the same person as the persons specified in the notification, the financial institution shall notify the notifying institution and the Financial Intelligence Unit of all identified persons.

25.15. Actions taken in the event of suspicion concerning identification of a subject of financial sanctions or a transaction or act violating financial sanctions:

25.15.1. If the employee of the obliged entity becomes aware that a person who is in business relationship or is performing a transaction or an act with them, as well as a person intending to establish a business relationship, perform a transaction or an act with them, is a subject of international financial sanction, the employee shall immediately notify the compliance officer or management board of the person having specific obligations, about the identification of the subject of international financial sanction, of the doubt thereof and of the measures taken.

25.15.1.1. The compliance officer or management board of the person having specific obligations shall refuse to conclude a transaction or proceeding, shall take measures provided for in the act on the imposition or implementation of an

international financial sanction and shall notify immediately the Financial Intelligence Unit of their doubts and of the measures taken.

25.15.1.2. When identifying the subject of an international financial sanction, it is necessary to identify the measures that are taken to sanction this person. These measures are described in the legal act implementing the sanction, therefore it is necessary to identify the exact sanction what is implemented against the person to ensure legal and proper application of measures.

25.15.2. If the employee of the person having specific obligations has doubts that a person who is in business relationship or is performing a transaction or an act with them, as well as a person intending to establish a business relationship, perform a transaction or an act with them, is a subject of international financial sanction, the employee shall immediately notify the compliance officer or management board of the person having specific obligations.

25.15.2.1. The compliance officer or management board of the person having specific obligations shall decide on whether to ask or acquire additional data from the person or notify the Financial Intelligence Unit immediately of their suspicion.

25.15.2.2. If, after the acquiring of the additional data and/or delivery of data by the person, the suspicion does not remain, the person having specific obligations shall not create additional obstacles for customers against whom there are no suspicions remaining.

25.15.2.3. If a person who is in a business relationship or is performing a transaction or an act with the person having specific obligations, as well as a person intending to establish a business relationship, perform a transaction or an act with them, refuses to provide additional information, or it can not be used to ascertain whether the person is a subject of international financial sanction, the person having specific obligations or their representative shall refuse to perform the transaction or act, shall take measures provided for in the act on the imposition or implementation of an international financial sanction and shall notify immediately the Financial Intelligence Unit of their doubts and of the measures taken.

25.16. Actions taken by the person having specific obligations regarding the identification of the risk of a breach of financial sanctions and the action to be taken in the event of such a finding:

25.16.1. In the opinion of the obliged entity, there is a higher risk of violation of international sanctions if the person who is in a business relationship with the obliged entity or wishes to establish a business relationship with the obliged entity or who performs transactions with the obliged entity during the business relationship:

25.16.1.1. is from a country which is subject to European Union and/or UN sanctions;

25.16.1.2. has inadequate data available or these data are presented in a shortened manner;

25.16.1.3. during the description of parameters of the inquiry made during the identification, some factors distorting personal data exist.

25.16.2. In the emergence of aforementioned circumstances, the obliged entity shall perform additional due diligence by applying enhanced due diligence measures.

25.17. Actions taken by the person having specific obligations in the event of acquiring additional information:

25.17.1. The person having specific obligations shall primarily acquire additional information on their own about the person who is in business relationship or is performing a transaction or an act with them, as well as the person intending to establish a business relationship, perform a transaction or an act with them, preferring information from a credible and independent source.

25.17.2. If, for some reason, the information specified in previous clause is not available, the person having specific obligations shall ask the person who is in a business relationship or is performing a transaction or an act with them, as well as the person intending to establish a business relationship, perform a transaction or an act with them, whether the information is from a credible and independent source and assess the answer.

25.18. The actions taken by the person having specific obligations in the course of performing the obligation to report:

25.18.1. The person having specific obligations shall immediately inform the Financial Intelligence Unit of the persons identified as a result of the inquiry if they have a reason to believe or have a permanent suspicion that the mentioned person is the same person who is specified in the notification containing the international sanction.

25.18.2. A person having specific obligations or a person authorised to represent them shall refuse to enter into a transaction or act with the aforementioned persons and take measures provided for in legal acts establishing or implementing international financial sanctions.

25.18.3. The application of sanctions against the said persons shall be decided by the compliance officer or the management board of the person with specific obligations after receiving the relevant confirmation or precept from the Financial Intelligence Unit.

25.19. Preserving and making available the data by the person having specific obligations.

25.19.1. The person having specific obligations shall collect and preserve the following data for five years:

25.19.1.1. time of inspection;

25.19.1.2. the name of the person who carried out inspection;

25.19.1.3. the results of inspection;

25.19.1.4. the measures taken.

25.19.2. The person having special obligations shall store the data on an electronic data carrier and implement appropriate security measures for the secure storage of the stored data. The management board of the person having special obligations shall be liable for preserving the data.

25.19.3. The management board of the person having special obligations shall ensure that the stored data are available upon the receipt of a relevant query within the same working day or in the case of resting days, no later than within 24 hours.

25.20. If an act on the imposition or implementation of an international financial sanction is repealed, expires or is amended in such a manner that the implementation of the international financial sanction with regard to the subject of the international financial sanction is terminated wholly or partially, the employees of the person having specific obligations shall immediately terminate the implementation of the measure to the extent provided for in the act on the imposition or application of the international financial sanction.

25.21. Upon the delivery of the notification, the Financial Intelligence Unit shall check whether the subject of the financial sanction has been correctly identified and whether the measures have been applied in a lawful manner and shall provide relevant feedback immediately, but not later than within two working days.

25.22. The duties of the person liable for applying the international sanctions are performed by the compliance officer of the obliged entity, or if not available, the management board of the obliged entity.

25.23. The countries subject to the European Union sanctions can be checked on the following webpage: https://www.sanctionsmap.eu/#/main; the subjects of European Union and UN sanctions can be checked on the webpage of the Financial Intelligence Unit: https://www.politsei.ee/et/rahapesu/.

26. OBLIGED ENTITY'S DUTY TO REPORT

26.1. The obliged entity must report to the Financial Intelligence Unit on the activity or the circumstances that they identify in the course of economic activities and whereby:

26.1.1. 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. UTR or UAR);

26.1.2. in the case of which they suspect or know 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. STR or SAR);

26.1.3. in the case of which they 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. TFR);

26.1.4. in the case of which an attempt of the activity or circumstances specified in clause 26.1.1 to 26.1.3 is present.

26.2. The Financial Intelligence Unit must be notified:

26.2.1. by the obliged entity also about the circumstances of refusal of establishment of a business relationship or completing an occasional transaction on the basis of clause 24.1 and about the extraordinary termination of a business relationship on the basis of clause 24.9 (primarily a suspicious and unusual transaction or activity report, i.e. UAR);

26.2.2. by the obliged entity, except a credit institution, also about each transaction that has become known whereby a pecuniary obligation of over 32 000 euros or an equal sum in another currency is performed in cash, regardless of whether the transaction is made in a single payment or in several linked payments over a period of up to one year (primarily an amount-based report, i.e. CTR).

26.2.3. by credit institutions also about each foreign exchange transaction in cash that exceeds 32 000 euros if the credit institution does not have a business relationship with the person participating in the transaction (primarily an amount-based report, i.e. CTR).

26.3. The reports specified in clauses 26.1 and 26.2 must be made before the completion of the transaction if the obliged entity suspects or knows that money laundering or terrorist financing or related crimes are being committed (see also clause 24.12) and if said circumstances are identified before the completion of the transaction. 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 obliged entity is in contact with the Financial Intelligence Unit in order to identify such circumstances.

26.4. 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).

26.5. In addition to the situation specified in clause 26.3, the obliged entity 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 extraordinary termination of a business relationship.

26.6. In a situation where, in the case of a so-called amount-based report or a report arising from the establishment or extraordinary termination of a business relationship and in respect of the customer or the circumstances related to them, the obliged entity has identified the activity or circumstances specified in clause 26.1, the reporting obligation must also be performed within the meaning of clause 26.1, whereby this may also take place within the scope of the same report, but by making reference to different indicators.

26.7. If the basis for compliance with the reporting obligation of the obliged entity is not a suspicion of money laundering or terrorist financing, but a so-called 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 obliged entity 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.

26.8. The obliged entity immediately submits to the Financial Intelligence Unit all the information available to the obliged entity, which the Financial Intelligence Unit requested in its inquiry.

26.9. Where relevant, the Financial Intelligence Unit gives obliged entities feedback on their performance of the duty to report and on the use of the received information.

26.10. The place and form of performance of duty to report:

26.10.1. A report is submitted to the Financial Intelligence Unit of the contracting state of the European Economic Area on whose territory the obliged entity was established, is seated or provides the service.

26.10.2. A report is submitted via the online form of the Financial Intelligence Unit or via the X-road service.

26.10.3. The data used for identifying the person and verifying the submitted information and, if any, copies of the documents are added to the report.

26.10.4. Requirements for the contents and form of a notice submitted to the Financial Intelligence Unit and the guidelines for the submission of a report are established

by a regulation of the minister responsible for the field, which is added as an appendix to these guidelines.

26.11. The duty to report, which arises from this section, does not apply to a notary, enforcement officer, bankruptcy trustee, auditor, attorney or other legal service provider, provider of accounting services or provider of advisory services in the field of accounting or taxation where they assess the customer's legal situation, defend to represent the customer in court, intra-authority or other such proceedings, including where they advise the customer in a matter of initiation or prevention of proceedings, regardless of whether the information has been obtained before, during or after the proceedings.

26.12. The obliged entity, a structural unit of the obliged legal entity, a member of a management body and an employee is prohibited to inform a person, its beneficial owner, representative or third party about a report submitted on them to the Financial Intelligence Unit, a plan to submit such a report or the occurrence of reporting as well as about a precept made by the Financial Intelligence Unit based on §§ 57 and 58 of the RahaPTS or about the commencement of criminal proceedings. After a precept made by the Financial Intelligence Unit has been complied with, the obliged entity may inform a person that the Financial Intelligence Unit has restricted the use of the person's account or that another restriction has been imposed.

26.13. The prohibition provided for in clause 26.12 is not applied upon submission of information to:

26.13.1. competent supervisory authorities and law enforcement agencies;

26.13.2. credit institutions and financial institutions in between themselves where they are part of the same group;

26.13.3. institutions and branches that are part of the same group as the person specified in subclause 2 of this clause where the group applies group-wide procedural rules and principles in accordance with § 15 of the RahaPTS;

26.13.4. a third party who operates in the same legal person or structure as an obliged entity who is a notary, enforcement officer, bankruptcy trustee, auditor, attorney or other legal service provider, provider of accounting services or provider of advisory services in the field of accounting or taxation and whereby the legal person or structure has the same owners and management system where joint compliance is practiced.

26.14. The prohibition provided for in clause 26.12 does not apply to the exchange of information in a situation where it concerns the same person and the same transaction that involves two or more obliged entities that are credit institutions, financial institutions, enforcement officers, bankruptcy trustees, auditors, attorneys or other legal service providers, providers of accounting services or providers of advisory services in the field of accounting or taxation located 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, act in the same field of profession and requirements equal to those in force in Estonia are implemented for keeping their professional secrets and protecting personal data.

26.15. Where a notary, enforcement officer, bankruptcy trustee, auditor, attorney or other legal service provider, provider of accounting services or provider of advisory

services in the field of accounting or taxation convinces a customer to refrain from unlawful acts, it is not deemed violation of the prohibition provided for in this section.

26.16. The exchange of information regulated in this section must be retained in writing or in a form reproducible in writing for the next five years and information is submitted to the competent supervisory authority at its request.

27. REGISTERING, VERIFYING AND RETAINING DATA

27.1. The obliged entity must register and retain:

27.1.1. information about the circumstances of refusal of the establishment of a business relationship or the completing an occasional transaction by the obliged entity;

27.1.2. information if it is impossible to take the due diligence measures using information technology means;

27.1.3. 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 customer if the refusal is related to the application of due diligence measures by the obliged entity;

27.1.4. 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 obliged entity is capable of reproducing the aforementioned data during the five-year time period for data retention. The obliged entity 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 two sources;

27.1.5. the documents that serve as a basis for the establishment of the business relationship but not specified in clause 26.1.4, incl. the documents collected in the course of application of due diligence measures;

27.1.6. the transaction date or period and a description of the contents of the transaction;

27.1.7. also the following data in relation to transactions:

27.1.7.1. when making transactions with a representative of a civil law partnership, community or another association of persons that does not have the status of a legal entity, trust fund or trustee, the fact that the person has such status, an extract of the registry card or a certificate of the registrar of the register where the association of persons that does not have the status of a legal entity has been registered;

27.1.7.2. upon opening an account, the account type, number, currency and significant characteristics of the securities or other property;

27.1.7.3. upon acceptance of assets for depositing, the deposition number and the market price of the assets on the date of deposition or a detailed description of the assets where the market price of the assets cannot be determined;

27.1.7.4. upon renting or using a safe deposit box or a safe in a bank, the number of the safe deposit box or safe;

27.1.7.5. upon making a payment relating to shares, bonds or other securities, the type of the securities, the monetary value of the transaction, the currency and the account number;

27.1.7.6. upon entry into insurance contracts, the account number debited to the extent of the first insurance premium amount;

27.1.7.7. upon making a disbursement under an insurance contract, the account number that was credited to the extent of the disbursement amount;

27.1.7.8. in the case of payment intermediation, the details the communication of which is mandatory under Regulation (EU) No 2015/847 of the European Parliament and of the Council;

27.1.7.9. in the case of another transaction, the transaction amount, the currency and the account number;

27.1.8. data and documents collected in the course of monitoring the business relationship, incl. the documents collected in the course of application of due diligence measures (covering all analyses related to understanding transactions and measures for identifying the background and objective of complicated, high-value 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);

27.1.9. all of the correspondence related to the performance of the obligations arising from these guidelines and the RahaPTS;

27.1.10. the information that serves as a basis for the duty to report to the Financial Intelligence Unit;

27.1.11. data of suspicious or unusual transactions or circumstances of which the Financial Intelligence Unit was not notified;

27.1.12. information about the circumstances of termination of the business relationship because the application of due diligence measures is impossible.

27.2. The data arising from clause 24.1 (excl. clause 24.1.10) must be retained for 5 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 arising from point 24.1.10 must be retained for 5 years after the performance of the reporting obligation.

27.3. If the obliged entity makes, for the application of due diligence measures, a query to a database that forms part of the state's information system, the obligations of data retention will be deemed to have been performed if the information about making the electronic query to said register can be reproduced over a period of five years after the expiry of the business relationship or the completion of the occasional transaction.

27.4. The obliged entity 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.

27.5. 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.

27.5.1. The manner of retention of documents and data also covers the systematic retention of data. This covers, for example, the division of the documents and data collected in the course of due diligence measures applied upon the establishment of a business relationship chronologically, among others, and the retention of the documents and data collected in the course of the due diligence measures applied during the monitoring of the business relationship in a manner which makes it possible to quickly and understandably connect them with the concluded transactions (if necessary, give the documents titles and retain them chronologically).

27.6. Upon implementation of § 31 of the RahaPTS, the obliged entity retains the data of the document prescribed for the digital identification of a person, information on making an electronic inquiry to the identity documents database, and the audio and video recording of the procedure of identifying the person and verifying the person's identity for at least five years after termination of the business relationship.

27.7. The obliged entity implements all rules of protection of personal data upon application of the requirements arising from the RahaPTS.

27.8. The obliged entity is allowed to process personal data gathered upon implementation of the RahaPTS only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

27.9. The obliged entity submits information concerning the processing of personal data before establishing a business relationship or making an occasional transaction with them. General information on the duties and obligations of the obliged entity upon processing personal data for AML/CFT purposes is given among this information.

28. PROCEDURE FOR AVOIDING CONFLICT OF INTERESTS

28.1. The obliged entity and the employees of the obliged entity must avoid the conflict of interests and when this happens, immediately notify the higher management body or the compliance officer of the obliged entity.

28.2. The conflict of interests is understood as all the circumstances known to the obliged entity or its employees that may affect the decisions of making a transaction or establishing a business relationship and which do not correspond to the interests of the obliged entity or its customer.

28.3. To achieve the goal of avoiding the conflict of interests, the obliged entity shall collect and regularly update its employee data in order to identify their interests in the context of preventing money laundering and terrorist financing. The obliged entity collects the following data about each employee:

28.3.1. the birthplace and place of residence of the employee;

28.3.2. other job positions and contracts of the employee that they have in the context of the economic field;

28.3.3. the data regarding the close relatives of the employee (spouse, parents, children, siblings and their children): for each person, their birthplace, place of residence and place of work.

28.3.4. other data known to the employee which may indicate to the interests in the context of preventing money laundering and terrorist financing.

28.4. The failure of the employee to provide the data specified in clause 28.3 is considered to be a significant violation of the employment contract and may result in the extraordinary cancellation of the employment contract for reason arising from the employee.

28.5. The obliged entity identifies and analyses, inter alia, whether the persons directing customers to the obliged entity (e.g. agents, resellers, etc.) have any interests regarding the customer (e.g., provide them with legal services, accounting services, services providing the establishment of companies and other legal structures, etc.) which cause the conflict of interests between the person directing customers to the obliged entity and the customer.

28.6. In case of identifying a conflict of interests or circumstances indicating a conflict of interests, the obliged entity shall apply all necessary measures to prevent it. If it is impossible to prevent the conflict of interests, the obliged entity must not conclude any transactions or establish a business relationship.

29. TRAINING

29.1. The obliged entity ensures the training of the employees involved in the prevention of money laundering and terrorist financing as well as of the senior management, incl. the management board. Training must also be guaranteed to the persons to whom the obliged entity has outsourced activities. Employees means the employees of all risk management lines of defence.

29.2. Above all, the subjects of training must be informed about the requirements regulating the prevention of money laundering and terrorist financing in respect of the implementation of due diligence measures and reports on suspicions of money laundering. The training must give information about, inter alia, the following:

29.2.1. the principles specified in the risk appetite document of the obliged entity;

29.2.2. the risks arising from the activities of and services provided by the obliged entity, incl. risks foreseen in the future;

29.2.3. the obligations stipulated in the rules of procedure;

29.2.4. the contemporary methods of committing money laundering and terrorist financing and specific typologies/cases, and the risks associated with them;

29.2.5. how to recognise actions related to possible money laundering or terrorist financing, and guidelines on how to act in such situations.

29.3. Training must take place when the employee commences the performance of said duties and thereafter regularly or as necessary. The obliged entity combines explanatory and informational parts with possible assessments of knowledge during training if necessary.

29.4. The regularity of training depends on the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk

appetite and risks arising from activities of the obliged entity, but it usually takes place at least once a year. If necessary, employees are trained or informed more frequently, incl. when the rules of procedure change, there are significant changes in the risks arising from activities, new trends and methods of money laundering and terrorist financing are detected, etc.

29.4.1. The training and assessments of knowledge for the employees and other liable persons must take place at least once per year for each employee or liable person.

29.5. The obliged entity retains the details of the person that carried out the training and the participants, the training materials and, if appropriate, the results of the training (e.g. test results) in a format that can be reproduced in writing for at least two years after the training took place.

30. MONITORING COMPLIANCE WITH RULES OF PROCEDURE

30.1. Financial Intelligence Unit and/or other competent authorities and institutions appointed by relevant legislation shall exercise supervision over the compliance of the management board of the obliged entity with the Money Laundering and Terrorist Financing Prevention Act and legal acts issued on the basis thereof.

30.2. The management board of the company, the responsible member of the management board or, if available, the compliance officer, shall exercise supervision and monitoring over the compliance of the employees, structural units and the compliance officer of the obliged entity with the Money Laundering and Terrorist Financing Prevention Act and legal acts issued on the basis thereof.

30.3. The competence of the employees of the obliged entity over compliance with the requirements of the Money Laundering and Terrorist Financing Prevention Act and legal acts issued on the basis thereof:

30.3.1. only the employees who have been authorised by the management board or by the responsible member of the management board, and who have thoroughly examined the relevant legislation, information disclosed by competent authorities, these guidelines, and have adequate knowledge in the AML/KYC field, deal with and have decisive powers over the acts related to the performance of requirements and obligations of the RahaPTS and legal acts issued on the basis thereof, including dealing with and having decisive powers over the establishment and continuation of business relationships.

30.3.2. the employees and the heads of the structural units of the obliged entity shall communicate primarily with the compliance officer, if not available, then the responsible member of the management board, regarding the matters related to the performance of requirements and obligations of the RahaPTS and legal acts issued on the basis thereof. The responsible member of the management board shall always have the right to supervise the activity of the employees, heads of the structural units and the compliance officer of the obliged entity.

30.4. The essentials of the due diligence obligations of the employees and the heads of structural units of the obliged entity arising from the RahapPTS , the internal rules of procedure established by the management board of the obliged entity and the nature of the services provided by the obliged entity are as follows:

30.4.1. the employees and the heads of the structural units of the obliged entity shall strictly follow:

30.4.1.1. the International Sanctions Act (RSanS);
30.4.1.2. the Money Laundering and Terrorist Financing Prevention Act (RahaPTS);
30.4.1.3. the Directive (EU) 2015/849 of the European Parliament and of the Council;
30.4.1.4. the relevant guidelines and orders of the Financial Intelligence Unit and other competent authorities;
30.4.1.5. the internal rules of procedure and internal control rules issued by the management board of the obliged entity;
30.4.1.6. the relevant and lawful orders of the management board, the responsible member of the management board and the compliance officer of the obliged entity;
30.4.2. if the employee (or the head of a structural unit) becomes suspicious about the fulfilment of some criteria of due diligence measures or related criteria (or whether the concluding of the transaction or establishing a business relationship is allowed or not) – the employee (or the head of a structural unit) is obligated to immediately contact their immediate superior (the head of a structural unit, the compliance officer, the responsible member of the management board), stop the transaction or the business relationship until they receive a response and an order on how to act in this situation;
30.5. The obliged entity shall apply the following internal control system for the performance of the requirements of the RahaPTS, the legal acts issued on the basis thereof, and the internal rules of procedure and internal control rules:
30.5.1. The activity of the employees of the obliged entity is monitored and supervised by:
30.5.1.1. the head of the structural unit of the employee;
30.5.1.2. if the head of the structural unit of the employee is not available, the responsible member of the management board and/or the compliance officer;
30.5.1.3. the employee is obligated to forward all relevant data that concerns the customers of the obliged entity and the nature of business relationship established with them, including the customer's personal data, customer's transaction data, the results of the application of the due diligence measures and other important information, to the head of the structural unit of the employee, or if not available, the responsible member of the management board and/or the compliance officer no later than on the next working day following the gathering of data and finishing the application of the due diligence measures;
30.5.2. the activity of the head of the structural unit of the obliged entity is monitored and supervised by the responsible member of the management board and/or the compliance officer;
30.5.2.1. the head of the structural unit of the obliged entity is obligated to forward all relevant data gathered by them or the employees of their structural unit, that concern the customers of the obliged entity and the nature of the business relationships established with them, to the compliance officer and/or the responsible member of the management board with relevant reports at least once per month;
30.5.3. the compliance officer of the obliged entity, if it exists, is monitored and supervised by the responsible member of the management board or the management board;

30.5.3.1. the compliance officer verifies the relevant data forwarded by the employees and the heads of the structural units of the obliged entity that concern the customers of the obliged entity and the nature of the business relationships established with them, and organises the preserving of these data pursuant to RahaPTS and these guidelines. The compliance officer shall provide the responsible member of the management board with relevant reports at least once per quarter;

30.5.4. the obliged entity and the responsible member of the management board is monitored and supervised by the management board or the person, structural unit, or institution that is temporarily or permanently appointed by the general meeting of the shareholders;

30.5.4.1. if no compliance officer exists, the responsible member of the management board verifies the relevant data forwarded by the employees and the heads of the structural units of the obliged entity that concern the customers of the obliged entity and the nature of the business relationships established with them, and organises the preserving of these data pursuant to RahaPTS and these guidelines.

30.6. The compliance officer, the responsible member of the management board or the management board of the obliged entity are obligated to inform on an ongoing basis the company's employees of the changes in legislation, of new regulatory positions of the supervisory authorities, of the activities of the obliged entity, of the changes in the risk assessments and criteria arising from the customers or certain customer groups, of the change in the short- and long-term business doctrine of the company and of the separate viewpoints and instructions (that are the result of a market situation, political and economic situation, orders of the supervisory authorities, etc.) to perform the obligations arising from the RahaPTS. The aforementioned information and notices do not have to be prepared as appendices to these guidelines and may be delivered in meetings, via heads of structural units, via email or through oral communication, but regardless of the manner of delivery, it is obligatory to follow them and comply with them;

30.7. The violation of the obligation to apply the due diligence measures pursuant to the RahaPTS, the failure to follow the order of the management board or the compliance officer, the failure to inform the responsible member of the management board, the management board, the compliance officer, or the Financial Intelligence Unit either directly or via the head of a structural unit in the event of suspicion of money laundering or terrorist financing, is sufficient grounds for starting a disciplinary proceeding against the employee and/or head of the structural unit and to terminate the employment relationship;

30.8. The management board of the obliged entity shall ensure that the resources allocated for the performance of the obligations of the RahaPTS and these guidelines are adequate and that the employees directly related to the performance of the obligations of the RahaPTS work in such conditions where the obligations arising from the RahaPTS and these guidelines are fully known.

30.9. The obliged entity is not obligated to perform an internal audit, except for the cases when this is requested by the responsible member of the management board, the management board, the general meeting of the shareholders or if the performance of an internal audit is prescribed by law.

30.10. The internal audit assesses, inter alia, whether:

30.10.1. the management framework of the obliged entity for the prevention of money laundering and terrorist financing is adequate;

30.10.2. the existing principles and activities/procedures are still appropriate and in compliance with the requirements arising from law and international practices as well as regulative requirements, and with the risk appetite and strategy of the obliged entity;

30.10.3. the activities/procedures are in compliance with the applicable legislation and rules of procedure, and the resolutions of the managing body;

30.10.4. the activities/procedures are implemented correctly and efficiently;

30.10.5. the activities of the first line of defence and the second line of defence, via the compliance and risk management functions, that deal with the management of the risks arising from activities of and services provided by the obliged entity, is appropriate, of high quality and effective;

30.10.6. the methods of the obliged entity (as 'cross-obliged entity' methods and as a holistic view) are appropriate and adequate for the prevention of money laundering and terrorist financing, and they correspond to the organisation's needs and the expectations of supervisory authorities.

These internal rules of procedure and internal control rules for the prevention of money laundering and terrorist financing are accepted and approved by the resolution of the management board on 15.11.2020.

Member of the Management Board
Yiannis Tsoutsoukis

Signature: _____

31. FINANCIAL INTELLIGENCE UNIT CONTACT INFORMATION

Address:	Republic of Estonia, Harju County, Tallinn, Tööstuse 52, 10416
Main phone:	(+372) 612 3840
Fax:	(+372) 612 3845
E-mail:	rahapesu@politsei.ee
E-mail:	rab.jarelevalve@politsei.ee
Web:	https://www2.politsei.ee/et/organisatsioon/rahapesu/

32. MANDATORY WEB RESOURCES

Online form to submit a report to the Financial Intelligence Unit:
https://rabis-web.politsei.ee/#/
Search for EU and UN international sanctions subjects:
https://www.politsei.ee/et/rahapesu
Sanctions applied in the European Union:
https://www.sanctionsmap.eu/#/main
List of sanctions in effect:
http://eeas.europa.eu/cfsp/sanctions/docs/measures_en.pdf
Member states of the European Union and states of the European Economic Area:
http://elik.nlib.ee/pohifakte-euroopa-liidust/liikmesriigid-euroopa-majanduspiirkonna-riigid
List of high-risk countries:
http://www.fatf-gafi.org/countries/#high-risk
Samples for the apostilles of various countries:
http://eng.profperevod.ru//corporative/apostil/apsample/?url=eng/corporative/apostil/apsample/
Document validity check:
https://www.politsei.ee/et/teenused/e-paringud/dokumendi-kehtivuse-kontroll/
Public register of authentic travel and identity documents online:
http://www.consilium.europa.eu/prado/ET/prado-start-page.html
Resources for checking local politically exposed persons:
https://www.politsei.ee/et/kasulik-info
NameScan database for checking foreign politically exposed persons:
https://namescan.io/FreePEPCheck.aspx
Other useful information and web links
https://www.politsei.ee/et/kasulik-info

LIST OF APPENDICES

The following appendices form an integral part of these internal rules of procedure and internal control rules:

1. Instructions for identification and management of risks relating to the customer and its activities;

2. Model for the determination of the customer's risk profile

3. Risk and risk appetite arising from the activity of the obliged entity

4. Money Laundering and Terrorist Financing Prevention Act, RT I, 17.11.2017, 38

5. International Sanctions Act, RT I, 19.03.2019, 11

6. Directive (EU) 2015/849 of the European Parliament and of the Council, May 20 2015

7. Content and form of the report submitted to the Financial Intelligence Unit and instructions for submission of the report, RT I, 01.12.2017, 20

8. Form of the report submitted to the Financial Intelligence Unit

9. Instruction for the submission of the report to the Financial Intelligence Unit

10. Financial Intelligence Unit's guide to the application of international financial sanctions

11. Advisory guidelines of the Financial Intelligence Unit regarding the characteristics of transactions with a money laundering suspicion

12. Advisory guidelines of the Financial Intelligence Unit regarding the characteristics of terrorist financing

13. 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

14. A list of officials of foreign states whose power of attorney authenticated or certified is equal to a power of attorney authenticated by an Estonian notary, RT I, 10.11.2010, 5

15. Common position adopted by the European Union on equivalent third countries

APPENDIX 1. INSTRUCTIONS FOR IDENTIFICATION AND MANAGEMENT OF RISKS RELATING TO CUSTOMER AND ITS ACTIVITIES

The obliged entity must identify, assess and understand the risks related to money laundering and terrorist financing in their own as well as their customers' activities and apply measures to mitigate these risks.

The appliable measures must be proportionate to the degree of identified risk. In the course of a risk-based approach, the obliged entity must assess the probability of the risks becoming real and the consequences of such an event. When assessing the probability, the possibility of the occurrence of the relevant circumstances must be taken into account, including the possibility of potential risks that may affect the activities of both the customer and the service provider, and the possibility that the probability of the occurrence of this risk increases.

The obliged entity is obligated to prepare a risk assessment in order to identify, assess and analyse the risks related to their activity in regard to money laundering and terrorist financing and financial sanctions. The steps taken to identify, assess and analyse risks must be proportionate to the nature, size and level of complexity of the economic and professional activities of the obliged entity.

This model for the identification and management of risks relating to the customer and its activities is prepared to apply the obligations arising from clauses § 14 1) (2) and (6) of the RahaPTS in accordance with the general regulation provided by the Money Laundering and Terrorist Financing Prevention Act, the International Sanctions Act and the Directive (EU) 2015/849 of the European Parliament and of the Council and includes:

1) the model for the identification and management of the risks arising from the customer and their activities and the determination of the risk profile of the customer;
2) the model for the identification and management of the risks arising from the activities of the obliged entity, including the procedure of identification and management of the risks related to new and available technologies and services and products, including new or untraditional sale channels and new or developing technologies.

These instructions use the following risk scale:

A – low risk (1 risk point)

No influential risk factors exist in any risk category, the customer itself and the customer's activities are transparent and do not deviate from the usual activities, i.e. the activities of a reasonable and average person, in that field of activity, and there is no suspicion that the risk factors as a whole could lead to the realisation of the risk of money laundering or terrorist financing.

B – usual risk (2 risk points)

One or several risk factors exist in the risk category that deviate from the usual activities of a person acting in that field of activity, but the activity is still transparent and there is no suspicion that the risk factors as a whole could lead to the realisation of the risk of money laundering or terrorist financing.

C – high risk (3 risk points)

One or several risk factors exist in the risk category that as a whole grows suspicion of the transparency of the person and their activities, which causes the person to deviate from persons usually acting in that field of activity and it is at least possible that money laundering or terrorist financing is taking place.

The obliged entities must perform all due diligence measures. The extent of the implementation of the measures depends on the nature of the specific business relationship or transaction or the level of risk of the person or customer participating in the transaction or act, i.e. the "know your customer" principle must be followed. When determining and defining the risk levels of the customer or a person participating in the transaction, the obliged entity shall take into account, inter alia, the following risk categories:

I. CUSTOMER-RELATED RISK

1. RISK RELATED TO LEGAL NATURE OF CUSTOMER AND IDENTIFICATION OF BENEFICIAL OWNERS

A **Low risk** is when the customer is:

- a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the beneficial owner;
- a legal person governed by public law established in Estonia;
- a governmental authority or another authority performing public functions in Estonia or a contracting state of the European Economic Area;
- an institution of the European Union;
- a credit institution or financial institution acting on its own behalf or a credit institution or financial institution located in a contracting state of the European Economic Area or a third country, which in its country of location is subject to requirements equal to those established in Directive (EU) 2015/849 of the European Parliament and of the Council and subject to state supervision;

B **Usual risk** is when the customer is:

- a natural person;
- a company with a firm and transparent structure and data of management bodies and beneficial owners (OÜ, AS, UÜ, TÜ, TÜH, incl. the foreign versions of these forms of companies) that are not listed on a market;

- a non-profit association (MTÜ);

C **High risk** is when:

- the beneficial owner of the natural person is some third person;
- the customer is a legal entity of any form whose structure of the management bodies and/or beneficial owners is confusing and the relevant data is verified on the basis of the statement of the customer's representative and/or internal or non-public documents provided by the customer;
- the customer company, or the company related to the customer, has shareholders acting as a front or bearer shares;
- the ownership structure of the customer company seems, when considering the activities of the company, unusual or too complicated;
- the customer is a foundation, civil law partnership, trust, or common fund;
- the customer is a person registered in a low tax territory. The list of countries not considered a low tax territory is available at: https://www.emta.ee/et/ariklient/tulud-kulud-kaive-kasum/mitteresidendi-eesti-tulu-maksustamine/nimekiri-territooriumidest;
- the customer is a subject of European Union or UN sanctions, the list of which can be accessed on the home page of the Financial Intelligence Unit at: https://www.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/

2. RISK RELATED TO THE COUNTRIES OR GEOGRAPHIC TERRITORIES OR JURISDICTIONS

A **Low risk** is when:

- the customer is from or their place of residence or location (hereinafter location) is in the Republic of Estonia;
- the location of the customer is in another country of the European Union or the European Economic Area;
- the location of the customer is in a third equivalent country which is provided by the common position adopted by the European Union (Appendix 16), which include Australia, Brazil, Canada, Hongkong, India, Japan, South Korea, Mexico, Singapur, Switzerland, the Republic of South Africa, USA;

B **Usual risk** is when the location of the customer is in a third country not listed above, excluding a third high-risk country;

C **High risk** is considered in circumstances where the risk is primarily increased in such an event where the customer, person participating in a transaction or the transaction itself is related to a country or jurisdiction which, based on the trustworthy sources in the country like mutual assessments, detailed assessment reports or published follow-up reports, has no valid and efficient systems of the prevention of money laundering and terrorist financing. According to the Commission Delegated Regulation (EU) 2016/1675 (Appendix 13), the third high-risk countries include Afghanistan, Bosnia and

Herzegovina, Guyana, Iraq, Lao PDR , Syria, Uganda, Vanuatu, Yemen, Iran, and DPR Korea. The list of countries as determined by the FATF belonging to third high-risk countries is disclosed on the following webpage: http://www.fatf-gafi.org/countries/#high-risk. Additionally, the following countries or jurisdictions indicate of a high risk customer, person participating in a transaction or transaction itself:

- that, according to credible sources, have significant levels of corruption or other criminal activity. To assess this, the data of annual Corruption Perceptions Index (CPI), published by the Transparency International (TI), is used and high risk is indicated by the CPI result of 39 or lower. The published CPI data is available online: https://en.wikipedia.org/wiki/Corruption_Perceptions_Index;
- that are subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations. The list of EU sanctions for countries is available online: https://sanctionsmap.eu; the list of UN sanctions is available online https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list;
- that provide funding or support for terrorist activities. These countries include DPR Korea, Syria, Sudan and Iran and they are primarily defined by the data of the United States State Department which is available online https://www.state.gov/j/ct/list/c14151.htm;
- that have designated terrorist organisations operating within their territory, as identified by the European Union or the United Nations. These countries primarily include Syria, Iraq, Libya, Sudan, Somalia, Nigeria, Pakistan, India, Lebanon, Palestine, Sri Lanka, Philippines, Tajikistan, Uzbekistan, Yemen. The list of terrorist groups determined by the EU and UN is available online: https://en.wikipedia.org/wiki/List_of_designated_terrorist_groups.

3. RISK RELATED TO CUSTOMER'S ACTIVITY AND TO PROVIDED PRODUCTS OR SERVICES

A **Low risk** is when the customer is a person performing usual and normal economic and professional activities and the turnover of the financial instruments of the customer, or the planned turnover of the financial instruments, is significantly small and does not exceed 40 000 euros per one year;

B **Usual risk** is when the customer is a person performing usual and normal economic and professional activities and the turnover of the financial instruments of the customer, or the planned turnover of the financial instruments, exceeds 40 000 euros per one year;

C **High risk** is when the business relationship takes place under unusual circumstances, including when the transactions are complicated and have unusually large scale, when the transaction patterns are unusal, or when the customer is a legal entity or another association of persons that does not have the status of a legal entity, if their economic activity does not have a reasonable and clear economic or lawful objective or it is not

characteristic of a specific business field or if the customer's activity includes any of the following, regardless of the amount of the turnover:

- private or personal banking;
- providing or intermediating a product or service which may promote anonymity;
- personal asset holding;
- undertaking handling large amounts of cash;
- currency exchange, conversion transactions;
- providing a service of exchanging a virtual currency against a fiat currency or a virtual currency wallet service;
- providing gambling services (in a casino, on the internet or at sports events);
- purchasing and selling gold (incl. scrap gold), other precious metals or gemstones;
- purchasing and selling luxury goods;
- providing internet advertising;
- providing innovative services;
- establishing, selling and managing companies;
- other activities with a higher than usual risk of money laundering or terrorist financing;
- customer is providing services via untraditional sales channels;
- there is a constant change of customers;
- the person's customer base has grown rapidly;

4. RISK RELATED TO BILLING AND TRANSACTIONS

A **Low risk** is when:

- a long-term contract is entered into with the customer that is in a written or electronic format or in a format that can be reproduced in writing;
- the obliged entity receives payments within the scope of the business relationship only via an account located in a credit institution entered in the Commercial Register in Estonia or in a branch of a foreign credit institution or in a credit institution that has been established or whose place of business is in a contracting state of the European Economic Area or in a state where requirements equal to those established in the Directive (ELU) 2015/849 of the European Parliament and of the Council are implemented;
- the total value of the incoming or outgoing payments of transactions made in the business relationship does not exceed 15 000 euros per year.

B **Usual risk** is when the customer uses the following during transactions with the obliged entity:

- a limited amount of cash that does not exceed 32 000 euros or the equal amount in another currency, regardless of whether the transaction is made as one payment or as several connected payments within a period of up to one year;

- a credit institution, financial institution, payment institution or a payment system that is not located in a high-risk third country or promoting anonymity and that is, according to its own experience or independent sources, reliable, and performs controls against money laundering and terrorist financing;

C **High risk** is when the customer uses the following during transactions with the obliged entity:

- credit institution, financial institution, paying insitution or tax system that promotes anonymity;
- credit institution, financial institution, paying insitution or tax system that is located in a high-risk third country;
- settlement channels and accounts belonging to unknown or unrelated third persons;
- settlement channels and accounts belonging to third persons who are unknown or unrelated;
- large amounts of cash that exceeds 32 000 euros or the equivalent sum in another currency, regardless of whether the transaction is made as one payment or as several connected payments within a period of up to one year;

5. RISK ARISING FROM POLITICALLY EXPOSED PERSON

A **Low risk** is when the customer is not a politically exposed person, the family member of the politically exposed person or a person known to be the close associate of the customer who is a politically exposed person;

B **Usual risk** is when the customer is a politically exposed person, the family member of the politically exposed person or a person known to be the close associate of the customer. In such a case, the due diligence measures provided for in section 41 of the RahaPTS are applied in addition to the usual due diligence measures. The background of the customer is verified primarily by:

- the customer providing the information and their statement;
- using the Google search engine, searching by the Latin name of the customer with their birth date;
- using the information avaliable at the web page of the Financial Intelligence Unit: https://www.politsei.ee/et/organisatsioon/rahapesu/kasulikku/

C **High risk** is when the customer is a politically exposed person, the family member of the politically exposed person or a person known to be the close associate of the customer. In such a case, the due diligence measures provided for in section 41 of the RahaPTS are applied in addition to the usual due diligence measures. The background of the customer is verified primarily by:

- the information and statements received from the customer;

- using the NameScan database at: https://namescan.io/FreePEPCheck.aspx, which is open access, and, if possible, any of the paid databases (e.g. Thomson Reuters, MemberCheck etc.);
- using Google and the local search engine of the customer's country of origin, if any, by entering the customer's name in both Latin and local alphabet with the customer's date of birth.
- using the local politically exposed persons database, if it exists. For example, the local politically exposed persons of Ukraine are available at: https://pep.org.ua/en/.

6. RISK RELATED TO IDENTIFICATION OF CUSTOMER.

A **Low risk** is when:

- the natural person who is the resident of the Republic of Estonia is identified face-to-face on the basis of documents provided for in subsection § 21 (3) of the RahaPTS;
- the customer who is a legal entity entered in the commercial register of the Republic of Estonia, or the register of non-profit associations and foundations, is identified on the basis of original documents provided for in subsection § 22 (3) of the RahaPTS or on the basis of the public information of the commercial register, or the register of non-profit associations and foundations face-to-face with the customer or the representative of the customer by identifying the representative on the basis of documents provided for in subsection § 21 (3) of the RahaPTS, and in the case of an authorised person, on the basis of a notarised or equivalent document certifying their authority, which has been legalised or certified by a certificate (apostille) replacing legalisation, unless otherwise provided for in an international agreement.

B **Usual risk** is when:

- the foreign natural person customer is identified face-to-face on the basis of documents provided for in subsection § 21 (3) of the RahaPTS;
- the foreign customer who is a legal entity is identified on the basis of original documents provided for in subsection § 22 (3) of the RahaPTS or on the basis of the public information of the commercial register, or the register of non-profit associations and foundations face-to-face with the customer or the representative of the customer by identifying the representative on the basis of documents provided for in subsection § 21 (3) of the RahaPTS, and in the case of an authorised person, on the basis of a notarised or equivalent document certifying their authority, which has been legalised or certified by a certificate (apostille) replacing legalisation, unless otherwise provided for in an international agreement.
- The identity of a natural person or legal entity is verified by a notarised or officially certified copy of the documents provided for in § 21 (3) of the RahaPTS or § 22 (3) of the RahaPTS.

C **High risk** is when:

- during establishing the identity or verifying the information provided, suspicion has arisen as to the reality of the information provided or the authenticity of the documents or the identification of the beneficial owner;
- a business relationship or transaction that is established or initiated in a manner whereby the customer, the customer's representative or party to the transaction is not met physically in the same place and whereby § 31 of the RahaPTS is not applied as a safeguard measure;
- the person is identified on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.
- the representative of the customer is a legal entity.

7. RISK RELATED TO CHANNELS OF COMMUNICATION OR TRANSMISSION BETWEEN THE OBLIGED ENTITY AND THE CUSTOMER.

A **Low risk** is when:

- the customer is communicated through a communication or mediation channel that is agreed upon at the start of the business relationship or transaction or reliably changed during the course of the business relationship;
- products or services are delivered to the customer through a reliably modified delivery channel during the business relationship or at the initiative of the transaction.

B **Usual risk** is when:

- at the start of the business relationship or transaction, the customer is communicated with through a temporary communication or mediation channel;
- the products or services are delivered to the customer through another temporary product or service delivery channel transmitted through an agreed communication or intermediation channel initiated by the business relationship or transaction.

C **High risk** is when:

- the customer is communicated through an accidental, unreliable or unusual communication or mediation channel;
- products or services are delivered to the customer through an accidental, unreliable or unusual delivery channel;
- the existence and nature of a risk factor associated with the service provider used to deliver the service or product being sold;
- the distance between the location of the customer and the service provided or product offered is significantly high;

Taking into account the above risk categories, the obliged entity must determine the risk level of the person involved in the transaction or the customer, for example whether the

customer's money laundering or terrorist financing risk is low, normal or high or corresponds to other risk levels specified and used by the obliged entity.

In order to determine the impact of each risk category, the obliged entity must assess the probability of the occurrence of risk factors in that risk category. To determine the impact of a particular risk category, a qualifying amount of the presence of risk factors that characterise it can be used to consider a particular risk factor as having “impact” or “no impact” for a given person when a certain threshold is exceeded.

Instructions for defining low level of risk:

- Generally, the customer's level of risk is low if there is no influential risk factor in any of the risk categories so it can be concluded that the customer and their activities do not have different characteristics from normal and transparent activities, and there is no doubt that the customer's activities may increase money laundering and terrorism financing.
- In the situations where due diligence is required by legal acts, and the information about the customer and its beneficial owner is publicly available, where the person's activities and transactions are consistent with their usual economic activity and do not differ from other similar customers' payments practises and behaviour, or where there are quantitative or other absolute restrictions, the obliged entity may consider the customer 's expected risk of money laundering or terrorist financing to be low.
- In the situation where at least one risk category qualifies as high, the risk of money laundering or terrorist financing cannot generally be low. On the contrary, low risk does not necessarily mean that the customer's activities cannot be linked to money laundering or terrorist financing.
- If the risk arising from the business relationship, the customer or the party to the transaction or the transaction is low, based on the risk levels assigned to the party or customer and other conditions provided for in RahaPTS are met, the obliged entity may apply simplified due diligence measures. In the case of simplified due diligence measures, the obliged entity may determine the extent of compliance with the due diligence measures.

Instructions for defining high level of risk:

- Generally, the customer's risk level can be considered high if, when assessing the risk categories as a whole, there is a suspicion that the customer’s activities are not usual or transparent, incl. there are influential risk factors and it can be assumed the risk of money laundering or terrorist financing is high or significantly increased. The customer’s risk level is also high if it is indicated by some separate feature of the risk factor. However, high risk does not necessarily mean that the customer is engaged in money laundering or terrorist financing.
- If the obliged entity considers the risk of the customer or the person involved in the transaction to be high, the obliged entity must apply enhanced due diligence

measures in order to properly manage the respective risks. The due diligence measures must be applied in accordance with the provisions of the RahaPTS.

The obliged entity shall document, update and disclose the determination of the level of risk to the competent authorities if necessary.

These internal rules of procedure and internal control rules for the prevention of money laundering and terrorist financing are accepted and approved by the resolution of the management board on 15.11.2020.

Member of the Management Board
Yiannis Tsoutsoukis

Signature: _____

APPENDIX 2. MODEL TO IDENTIFY RISK LEVEL OF CUSTOMER

These guidelines provide the table below to identify the customer's risk level, which contains the arithmetic method and formula used to determine the customer's risk level. This table is filled with the results of the customer analysis previously performed in accordance with this Appendix (1 to 3 risk points will be assigned to each aspect of the risk analysed).

RISK CATEGORIES:

1. Risk related to the legal nature of the customer and the identification of the beneficial owners
2. Risk related to the countries or geographical areas or jurisdictions
3. Risk related to the customer's activity and the provided products or services
4. Risk related to billing and transactions
5. Risk arising from a politically exposed person
6. Risk related to the identification of a customer
7. Risk related to the channels of communication or transmission between the obliged entity and the customer
8. Risk related to activities of obliged entity and nature of services provided

TABLE:

	Low (1 point)	**Medium (2 point)**	**High (3 point)**	**Coefficient**	**Result**
1 risk cat.				2	
2 risk cat.				1	
3 risk cat.				2	
4 risk cat.				1	
5 risk cat.				1	
6 risk cat.				1	
7 risk cat.				1	
8 risk cat.				1	
The parameters for determining the risk level of customer are: **A.** The risk level of the customer is **low**, if **x < 2** **B.** The risk level of the customer is **medium**, if **2 ≤ x ≤ 2,75**				**Average result (x):** **Risk level of the customer:**	

C. The risk level of the customer is **high**, if **x > 2,75**		

NB! Even if the average result of the customer's level of risk indicates a low risk category it is not a customer with a low risk category if at least one of the categories indicates high risk. The customer's general risk category is high even if it is indicated by some separate risk factor.

These internal rules of procedure and internal control rules for the prevention of money laundering and terrorist financing are accepted and approved by the resolution of the management board on 15.11.2020.

Member of the Management Board
Yiannis Tsoutsoukis

Signature:_____

APPENDIX 3. RISK AND RISK APPETITE ARISING FROM ACTIVITIES OF OBLIGED ENTITY

The economic activity of the obliged entity as the provider of a virtual currency service is primarily related to the handling and storage of currencies presented in a digital form. The provision of a service of exchanging a virtual currency against a fiat currency and a virtual currency wallet service primarily requires the use of new and evolving technologies, which may involve the implementation of new or non-traditional sales channels in the economic activities of the obliged entity.

The vast majority of virtual currencies are comprised of different cryptocurrencies and related tokens, built on a new and rapidly evolving blockchain technology and a distributed database that is updated through a mathematical consensus algorithm.

It is the opinion of the management board of the obliged entity that the activities of the service of exchanging a virtual currency against a fiat currency and a virtual currency wallet service have a higher-than-usual risk level of activity within the meaning of RahaPTS. This assessment is mainly the result of the following factors:

1) Block-chain technology is new and evolving, so the mechanisms and algorithms for its occurrence, existence, transfer and trading are not constant and may be too complex to understand. This encourages the involvement and use of virtual currencies, including cryptocurrency, in various fraudulent schemes and scams;
2) Block-chain technology promotes anonymity (cryptocurrency wallet addresses are not personalised and exist usually in large quantities), which may involve the use of virtual currencies, including cryptocurrency, in money laundering, tax evasion, terrorist financing or criminal schemes;
3) Block-chain technology is based on a P2P network and is not regulated by any central organisations which may facilitate the manipulation of the value of virtual currencies, including cryptocurrency.

This risk analysis, risk mitigation method and the definition of risk appetite arising from the activities of the obliged entity as a provider of service of exchanging a virtual currency against a fiat currency and a virtual currency wallet service have been prepared in order to fulfil the obligation arising from the RahaPTS in view of the general risk associated with the obliged entity’s activities.

The management board of the obliged entity obligates to inform the employees of the company on an ongoing basis about changes in the risk assessment arising from the obliged entity’s activities and changes in the company's long-term and short-term doctrine and separate viewpoints and instructions (according to the market situation, the political and economic situation, the arrangements of the supervisory authorities, etc) in order to comply with the provisions of the RahaPTS. This information and these notices do not necessarily have to be in the form of appendices to these guidelines and may be provided at meetings,

through the heads of structural units, via e-mail or orally, but regardless of the method of transmission, it is mandatory to comply with and follow this information and these notices.

I. RISK RELATED TO ACTIVITIES OF OBLIGED ENTITY AND NATURE OF SERVICES PROVIDED

The following lists the risk factors and circumstances related to the customer's degree of risk arising from the nature and volume of services provided by the obliged entity to the customer.

A **Low risk** is when:

- the obliged entity sells any virtual currency to the customer and the customer pays for it through a payment account located in a credit institution, electronic money institution or payment institution established in Estonia.
- the obliged entity provides the customer with a virtual currency wallet service and the customer keeps in their virtual currency wallet their own virtual currency, which was purchased from the obliged entity does not transfer these virtual currencies to third parties or receive virtual currency transfers from third parties;
- the total value of incoming or outgoing payments for business transactions does not exceed 15 000 euros per year.

B **Usual risk** is when:

- the obliged entity sells any virtual currency to the customer and the customer pays for it through a payment account located in a credit institution, electronic money institution or payment institution established in Estonia or in a contractual state of the European Economic Area.
- the obliged entity provides the customer with a virtual currency wallet service and the customer keeps their virtual currency in the virtual currency wallet and makes virtual currency transfers to virtual currency wallets opened in an institution subject to requirements equivalent to RahaPTS;
- the total amount of incoming or outgoing payments related to business transactions or service contract in one calendar month does not exceed 15 000 euros for a natural person and 25 000 euros for a legal entity.

C **High risk** is when:

- the obliged entity sells any virtual currency to the customer and the customer pays for it through a payment account located in a credit institution, electronic money institution or payment institution established outside of a contractual state of the European Economic Area.
- the customer sells and the obliged entity purchases virtual currency for money which promotes anonymity;
- the obliged entity provides the customer with a virtual currency wallet service and the customer keeps their virtual currency in the virtual currency wallet and

transfers virtual currencies to virtual currency wallets opened in an institution for which no requirements equivalent to RahaPTS have been established;

- the obliged entity provides the customer with a virtual currency wallet service and the customer keeps the virtual currency of third parties in the virtual currency wallet;
- the total amount of incoming or outgoing payments related to business transactions or service contract in one calendar month exceeds 15 000 euros for a natural person and 25 000 euros for a legal entity.

II. MITIGATION OF RISKS

Given that money laundering, terrorist financing and support for criminal activities generally has a cause and is effective when dealing with larger amounts of money than usual, the obliged entity shall, in addition to the due diligence measures set out in these guidelines, impose the following restrictions on the volume of business transactions:

1. If the results of a customer risk analysis allows for the application of simplified customer due diligence measures, they may be applied to a customer whose total value of incoming or outgoing payments does not exceed 1000 euros per year, and the value of monthly payments does not exceed 500 euros;
2. If the results of a customer risk analysis allows for the application of usual customer due diligence measures, they may be applied to a customer whose total value of incoming or outgoing payments does not exceed 15 000 euros per year, and the value of monthly payments does not exceed 5000 euros;
3. If the total value of incoming or outgoing payments in the course of a customer's business relationship exceeds 15 000 euros per year, that customer shall always be subject to enhanced due diligence measures.
4. If the total value of incoming or outgoing payments in the course of a customer's business relationship exceeds 100 000 euros per year, the compliance officer of the obliged entity or, if not available, the responsible member of the management board shall decide on the establishment or continuation of this customer’s business relationship.

III. RISK APPETITE

In conjunction with the risk mitigation system established in this appendix and the provisions of the customer risk identification model (Appendix 2), the management board of the obliged entity determines the risk appetite of the obliged entity as usual.

The obliged entity shall not enter into business relations with persons who are prohibited by these guidelines and its appendices or laws and/or who are suspected by the obliged entity of using the obliged entity’s services for money laundering, tax evasion, terrorist financing or

criminal schemes, but shall not create additional barriers to the use of services by customers for whom there are no such doubts.

The obliged entity shall avoid business relations in particular with the following categories of customers:

1. It is not possible to identify the customer;
2. It is not possible to apply the due diligence measures arising from RahaPTS to the customer for any reason;
3. The customer is located in a high-risk third country as referred to in Directive (EU) 2015/849 of the European Parliament and of the Council;
4. The customer is a subject of the European Union or UN sanctions;
5. The customer is a legal entity of any form whose structure of the management bodies and/or beneficial owners is confusing and the relevant data cannot be verified, including on the basis of the statement of the customer's representative and/or internal or non-public documents provided by the customer;
6. The customer has previously been convicted of money laundering, tax evasion, terrorist financing or criminal activities that may be directly or indirectly linked to virtual currencies or is under criminal proceedings and the obliged entity has information in this regard.

For other customers with whom the obliged entity does not exclude the establishment of a business relationship, the obliged entity shall establish for the risk mitigation the due diligence measures in accordance with RahaPTS and these guidelines and procedures according to the customer's risk level, by assessing the customer's overall risk level using the risk assessment and management model set out in this Appendix and by turning attention to each risk category of the customer.

IV. CUSTOMER IDENTIFICATION SPECIFICATIONS

The obliged entity may establish the identity of a customer, in addition to the provisions provided for in § 21 (3) or § 22 (3) of the RahaPTS which require meeting the customer face-to-face, in such a way that enables identification of the customer without being in the same place. In such a case, the customer shall deliver the original identity document to the obliged entity in the form that is authenticated by a notary or certified by a notary or officially.

Alternatively, the possibility provided for in § 21 (4) or § 22 (4) of the RahaPTS shall be used to identify the customer on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.

The obliged entity shall mainly use two sources from the following list:

1. The customer shall be interviewed by means of an information technology device established and implemented by the obliged entity which is secure and does not allow data processing and which allows the transmission of a synchronised audio and video stream, in which the customer demonstrates their identity document and face in such a way that all the data is legible and a high quality photograph of the customer's document and face can be taken. The aforementioned interview and the photos taken are recorded and kept under the conditions set forth by the provisions of RahaPTS;
2. The customer makes a trial payment (for example in the amount of 1 euro) to the obliged entity from an account located in a credit institution registered in Estonia or a branch of a foreign credit institution that is established or the seat of which is in a contracting state of the European Economic Area or in a country applying requirements equivalent to the Directive (EU) 2015/849 of the European Parliament and of the Council;
3. The customer shall transmit to the obliged entity, through an information technology device established and put into use by the obliged entity which is secure and does not allow data processing, images of their identity document and face in such a way that all the data is legible and a high quality photograph of the customer's document and face can be taken. The aforementioned photos taken are recorded and kept under the conditions set forth by the provisions of RahaPTS;
4. The customer delivers to the obliged entity in a digital form a picture of the customer's rent, utilities, gas, electricity, telephone or internet bill that has been paid for, through which it is possible to identify the customer's personal data along with the address of residence;
5. The customer delivers to the obliged entity in a digital form a statement of their bank account, which is confirmed by the bank and from which the customer's personal data with the address of residence can be seen;

The procedures containing additional details for the customer identification based on the information from other reliable and independent sources shall be established in the rules of procedure.

V. VOLUME AND EXTENT OF PRODUCTS AND SERVICES OFFERED DURING BUSINESS ACTIVITY

The obliged entity sells products and provides services to customers, taking into account the customer's risk profile. Thus, some of the products or services provided by the obliged entity may be offered to the customer either partially, with certain restrictions, or not at all.

These internal rules of procedure and internal control rules for the prevention of money laundering and terrorist financing are accepted and approved by the resolution of the management board on 15.11.2020.

Member of the Management Board
Yiannis Tsoutsoukis

Signature:_____

INFORMING EMPLOYEES

I hereby confirm that I have examined the rules of procedure and the internal control rules to prevent laundering and terrorist financing, including their appendices, and I understand the requirements, obligations, rights and recommendations arising from law, rules and guidelines.

	First and last name of employee	Job title	Date of reading these rules
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			