

**BaGuk Finance OÜ**

**Rules of Procedure**

**for prevention of money laundering and terrorism  
and for the application of an international sanction**

## Table of contents

1. Introduction .....	3
2. Terms.....	4
3. Risk management.....	7
4. Procedures for applying customer due diligence .....	13
5. Transfer of business .....	25
6. Procedure for collecting and storing data.....	27
7. Compliance with the notification procedure .....	29
8. Procedure for inspecting compliance with the Guideline.....	31

## 1. Introduction

These rules of procedure for the prevention of money laundering and terrorist financing and for the application of an international sanction (hereinafter the **Guideline**) have been drafted in accordance with the general requirements and provisions of § 14 of the Money Laundering and Terrorist Financing Prevention Act (hereinafter the AML/CFT Act) and § 13 (6) the International Sanctions Act, in addition to the provisions of the advisory guidelines established by the Financial Supervision Authority on July 3, 2013.<sup>1</sup>

---

<sup>1</sup> In the computer network: [http://www.fi.ee/failid/Soovituslik\\_juhend\\_Rahapesu\\_tokestamine.pdf](http://www.fi.ee/failid/Soovituslik_juhend_Rahapesu_tokestamine.pdf)

## 2. Terms

The following terms used in this Guideline have the following meaning :

**Personal data form** means the private limited company (PLC) form used for the identification of the person and the beneficial owner.

**Financial service provider** means the PLC within the meaning of this Guideline.

**Financial service** means the provision of exchange services whereas customers are able to perform any conversion from Digital Assets into fiat money and vice versa.

**Beneficial owner** means a natural person who exercises control over a transaction, deed or another person, and in whose interest or for whose profit or at whose expense the transaction or deed is performed. The beneficial owner means a natural person who holds shares or voting rights of a business undertaking or exercises final control over the management of the business undertaking, either holding more than 25% of the shares or voting rights through direct or indirect ownership or control, including in the form of bearer shares, or by controlling the management of the legal entity in another way. The beneficial owner is also deemed to be a natural person who is the beneficial owner of a property of a legal person, partnership or other similar contractual legal entity engaged in the management or distribution of an asset for at least 25% as previously determined or who substantially controls a legal person, partnership or other such contractual legal entity's assets for at least 25 percent. In the case of a limited partnership fund, partnership, community or association of persons who do not have the status of a legal entity, the beneficial owner is the natural person who directly or indirectly owns or otherwise directly or indirectly controls the association and is the association's (i) founder or a person who has transferred assets into the asset pool; (ii) trustee, asset manager or possessor; (iii) the person providing and controlling the maintenance of the property, if such a person has been designated; or (iv) the beneficial owner or, if the beneficial owner (s) are designated in the future, the circle of persons in whose interest such an association was primarily established or operates.

**Terrorist financing** means the allocation or collection of funds for the planning or commission of acts deemed to be terrorism (Penal Code Chapter 15, Section 3) or terrorist organizations, or knowing that these funds are used for the aforementioned purpose.

**Money laundering** means the concealment or disguise of the true nature, source, location, disposition, movement, right of ownership or other rights related to property derived from criminal activity or property obtained instead of such property. This term also includes the conversion, transfer, acquisition, possession or use of property derived from criminal activity or property obtained instead of such property for the purpose of concealing or disguising the illicit origin of the property or of assisting a person who is involved in criminal activity to evade the legal consequences of his or her action. Money laundering is also participation in the aforementioned activities, association with such activities, attempts to commit an act, and aiding and abetting or encouraging or advising. Money laundering also means a situation whereby the criminal activity that generated the property to be laundered was carried out in the territory of another state.

**Financial Intelligence Unit (RAB)** means an independent structural unit of the Police and Border Guard Board whose main task is to prevent money laundering and terrorist financing in Estonia. RAB analyzes and verifies the information received from obligated subjects and other parties about suspicion of money laundering or terrorist financing, if necessary, takes measures to preserve the asset, and promptly sends the material to competent authorities when discovering the features of the crime.<sup>2</sup>

---

<sup>2</sup> Contact data of the Financial Intelligence Unit:

**Contact Person** means the RAB contact person appointed by the board of the Financial Services Authority. Only a person who has the necessary education, professional suitability, capabilities, personal qualities, experience and impeccable reputation for the fulfilment of the tasks of the contact person can be appointed a contact person. The tasks of a contact person may be filled by an employee or a structural unit. If the tasks of the contact person are performed by the structural unit, the head of the respective structural unit shall be responsible for the fulfilment of these tasks. A contact person designated by the management board of the financial service provider is also **responsible for the application of the international financial sanction**.

**Customer** means any natural or legal person who uses or has used the financial services offered by the PLC. The measures applicable in these Guideline to the customers of this PLC, if applicable, apply also to the applicants of Financial service.

**Politically exposed person** means a natural person who performs or has performed significant duties of public authority, as well as family members and close associates of such a person. A person who has not performed significant duties of public authority, or the family members and close associates of such a person are not regarded politically exposed persons.

The person carrying out significant duties of public authority is:

- Head of State, Head of Government, Minister and Deputy Minister;
- Member of the Parliament;
- Judge of the Supreme Court, the Constitutional Court and other such higher court whose decisions can be appealed only in exceptional cases;
- Member of the national audit Office and council of the central bank;
- An ambassador, an attorney, an officer who has a military rank in the subcategory of a senior officer;
- Member of the management, supervisory and administrative body of a state company.

The above list also covers the positions of the European Union and other international organizations.

A family member of the person carrying out significant duties of public authority is:

- his/her spouse;
- a partner equivalent to the spouse, in accordance with the law of the country of residence or a person who has had at least one year's common household with him/her as at the date of conclusion of the transaction;
- her children and their spouses or partners within the meaning of the preceding paragraph;
- his/her parent.

A close associate of a person performing significant duties of public authority is:

- a natural person who has close business relations with the person performing significant duties of public authority or who together with the person performing significant duties of public authority is the joint beneficial owner of a legal person or contractual legal entity;
- a person who, as the beneficial owner, fully owns a legal person or contractual legal entity that is known to have been established for the benefit of a person performing significant duties of public authority.

**Risk appetite** means the set of risks and types of risks of the Financial Services Provider that the latter is prepared to undertake in the course of its business in order to implement economic activities and strategic objectives. The risk appetite is confirmed in writing by the management board of the Financial Services Provider.

**Tax-exempt territory or territory with low tax rate** means a territory with a minimum or no tax liability for persons registered there. There is no official list of countries that are considered low tax

rates. The definition of low tax rates must be based on Regulation No. 55 of the Minister of Finance of 18.12.2014 "List of territories which are not regarded low-tax territories"<sup>3</sup>.

**International sanction** is a measure which is not related to the use of the armed forces and which the European Union, the United Nations, other international organizations or the Government of the Republic have decided to establish in order to maintain or restore peace, to prevent conflicts and to strengthen international security, to support and consolidate democracy, to observe the rule of law, human rights and international law and to achieve other objectives of the European Union's Common Foreign and Security Policy.

**Subject of an international sanction** means a state, a specific territory, territorial unit, regime, organization, association or group, subject to the measures provided for by an instrument imposing an international sanction; as well as any natural or legal person, institution, partnership or any other entity expressly mentioned in an international instrument imposing or enforcing a sanction and subject to the measures provided for by an instrument imposing an international sanction.<sup>4</sup>

**A high-risk third country** means a country as referred to in the delegated act adopted under Article 9 (2) of European Parliament and Council Directive (EU) 2015/849. The list of high risk third countries is available here: <http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016R1675&from=ES>.

**Business relationship** within the meaning of this Guideline means the relationship between OÜ and its customer which occurs upon the conclusion of a credit agreement.

**Reliable source** includes, among others, data from the registers of the respective state or documentation issued by public authorities. In assessing a document the main criterion for reliability is its authenticity or notarised certification of the copy of the original document, as well as the time and/or place of its issuance or compilation may be the reliability indicator of the document. Electronic online or other public sources may be used to identify or verify the beneficial owner(s) of the transaction.

#### **Field of activity and the activity profile of a customer as legal person**

In establishing a business relationship with a legal entity that is a customer of a financial institution, the employee in charge must identify the customer's area of activity and the activity profile that would allow to assess the circumstances indicating money laundering or terrorist financing in the activities of customer. The employee in charge, among others, identifies the customer's permanent places of business in a third country, key business partners and payment practices, taking into account the specifics of the activities of the financial institution.

In the event that the field of activity of the legal person can not be convincingly identified on the basis of the testimony of the customer or the customer's representative, the employee in charge must contact public sources (Register of Economic Activities (MTR), Commercial Register, published annual reports, Internet search engines, information registers) and verify and, if necessary, update the information provided.

---

<sup>3</sup> Available online at <https://www.riigiteataja.ee/akt/119122014015>

<sup>4</sup> The list is updated regularly and is available online at <https://www.politsei.ee/et/organisatsioon/rahapesu/finantssanktsiooni-subjekti-otsing-ja-muudatused-sanktsioonide-nimekirjas/>

### **3. Risk management**

#### **3.1. Risk assessment and risk appetite**

- 3.1.1. The management board of the Financial Service Provider, together with the Contact Person and, if necessary, other employees who in their daily work are exposed to the mitigation of the risks of combating money laundering and terrorist financing, will prepare a risk assessment for identifying, assessing and analyzing the risks associated with money laundering and terrorist financing.
- 3.1.2. When preparing the risk assessment, the Financial Service Provider maps out the risks associated with money laundering and terrorist financing related to its activities, taking into account the risk categories mentioned in clause 3.2. The effects of mapped risks are then assessed for the activities of the Financial Services Provider and possible countermeasures that can hedge the risks mapped, their reasonableness and the applicability are analysed.
- 3.1.3. As a result of the risk assessment, the Financial Service Provider determines:
  - 3.1.3.1. Fields with smaller and larger money laundering and terrorist financing risks;
  - 3.1.3.2. Risk appetite, including the scope and extent of the products and services offered in the course of business;
  - 3.1.3.3. Risk management model for hedging the identified risks.
- 3.1.4. The determination of risk appetite takes into account the risks which a Financial Service Provider is prepared to take or which he wishes to avoid in connection with his business and qualitative and quantitative compensation mechanisms such as planned revenue, measures taken with the help of capital or other liquid assets or other circumstances such as reputation risks and risks associated with money laundering and terrorism financing, or other unethical activities.
- 3.1.5. The management board of the Financial Service Provider determines whether business relations are intended to be created with persons from countries outside the European Economic Area..
- 3.1.6. The Financial Service Provider documents the risk assessment and determination of the Risk appetite, and update these documents as required, at least once every three years, and according to the results of the state risk assessment.

### 3.2. Risk categories and circumstances mitigating and increasing risk

3.2.1. When drawing up risk assessment and determining the customer's risk profile, the Financial Services Provider takes into account at least the following risk categories:

- 3.2.1.1. Customer risk;
- 3.2.1.2. Risk related to the country or geographic regions or jurisdictions;
- 3.2.1.3. Risk associated with products, services or transactions;
- 3.2.1.4. Risk associated with communication or brokerage channels between the Financial Service Provider and customers or transmission channels for products, services or transactions.

3.2.2. **Customer risk**, ie risk factors of the person or customer participating in the transaction, including:

- the legal form, management structure, field of activity of the person;
- whether it is a politically exposed person;
- whether the person is represented by a legal person;
- whether a third party (individual) is the beneficial owner;
- whether the identification of beneficial owners is impeded by complex and nontransparent ownership relations;
- whether the person is subject to an international sanction?
- the possibility of classifying the customer person as a typical customer of a certain customer category;
- circumstances (including suspicious transactions identified in the course of a prior business relationship) resulting from the experience of communicating with the person, its business partners, owners, representatives and any other such persons;
- the duration of the operations and the nature of business relationships;
- the type and characteristics of the service provided or product sold (whether the service or product is unusual or economically impracticable; whether the service or product may be related to crime or development of weapons of mass destruction; whether there is a considerable distance between the customer's seat and the destinations of the service or product; etc.);
- whether the person participates in transactions where cash plays a major role (e.g. currency exchange locations and gambling operators);
- whether the person's customers are the same or change constantly;
- whether the person's customer base has increased rapidly;
- whether the person renders the service to anonymous customers;
- the existence and nature of the risk factor relating to a service provider used to forward the service or product;
- the type and characteristics of the services used or products consumed by the person other than the obligated person;
- the nature of the personal activities of an individual;
- whether the origin of the person's assets or the source and origin of the funds used for a transaction can be easily identified;

3.2.2.1. **Circumstances increasing customer risk** are, above all, situations where:

- the business relationship operates in unusual circumstances, including complex and unusually large transactions and unusual transaction patterns that do not have a reasonable, clear economic or legal purpose or which are not specific to a particular business specificity;
- the customer is a resident of a higher risk geographical area listed in clause 3.2.3.1 of this Guideline;



- the customer is a legal entity or a non-legal personality association dealing with personal property management;
- the customer is an entrepreneur handling large amounts of cash;
- The customer or company related to it has shell shareholders or bearer shares;
- The ownership structure of the business undertaking as the customer seems unusual or too complicated in view of the company's operations.

3.2.2.2. **Circumstances reducing customer risk are**, in particular, situations in which the customer is:

- a company listed on a regulated market that is subject to disclosure requirements that imposes requirements to ensure sufficient transparency for the beneficial owner;
- a legal entity in public law established in Estonia;
- government or other public authority in Estonia or the contracting state of the European Economic Area;
- European Union Agency;
- a credit institution or a financial institution acting on its behalf, a credit institution or a financial institution located in a contracting state of the European Economic Area or a third country subject to equivalent requirements in the country of its establishment, the performance of which is subject to state supervision;
- a person who is a resident of a country or a geographical area who complies with the characteristics specified in clause 3.2.3.2 of the Guideline.

3.2.3. **Geographical risk**, ie the risk arising from differences in the legal environment of various countries to which the customer, customer's representative or beneficial owner is associated, including:

- whether the country applies legal provisions that are in compliance with the International
- standards of prevention of money laundering and terrorist financing
- whether there is a high crime rate (incl. drug-related crime rate) in the country;
- whether the country cooperates with a criminal group; whether criminal groups use the country to pursue their operations;
- whether the country engages in proliferation;
- whether there is high level of corruption in the country;
- whether international sanctions have been or are being imposed on the country;
- whether other measures have been taken against or positions of international organisations have been expressed..

3.2.3.1. **Circumstances increasing the geographical risk** are, in particular, situations where the customer, the person involved in the transaction, or the transaction itself is related to the state or jurisdiction:

- where, according to reliable sources such as peer reviews, detailed assessment reports or published follow-up reports, effective systems to prevent money laundering and terrorist financing have not been established;
- where, according to reliable sources, the level of corruption or other criminal activity is significant;
- which are subject to sanctions, embargoes or similar measures, for example by the European Union or the United Nations; which finance or support terrorism or on which territory terrorist organizations designated by the European Union or the United Nations operate.

3.2.3.2. **Circumstances reducing geographical risk** are, in particular, situations where the customer is from the following country or has his or her residence in the following country:

- in the European Economic Area;
- in a third country with effective systems for prevention of money laundering and terrorist financing;
- in a third country where, according to reliable sources, corruption and other criminal activity levels are low;
- in a third country which according to reliable sources such as peer reviews, reports or published follow-up reports, have established requirements for prevention of money laundering and terrorist financing in line with the amended recommendations of the Money Laundering Advisory Board and where these requirements are effectively applied.

3.2.4. **Product or service risk**, i.e. the customer's economic activity and the availability of the product or service offered by the customer may result in money laundering risks, including:

- private banking, personal banking;
- currency exchange, conversion transactions;
- alternative means of payment, electronic money intermediation;
- provision of gambling services in casinos, Internet and sports competitions;
- purchase and sale of gold, including rum, and gemstones;
- purchase and sale of precious goods;
- offering online advertising;
- provision of innovative services;
- establishing, selling, managing companies.

3.2.4.1. **The circumstances that increase the risk of product or service risk** are, in particular, the following situations:

- making or arranging a transaction that may promote anonymity;
- payments from unknown or unrelated third parties;
- business relationship or transaction that is created or initiated in a manner that is not located at the same place with the client, its representative office or the counterparty and the recognition of the misrepresentation is not detected by IT intermediaries;
- new products and new business practices, including the use of a new delivery mechanism or new or emerging technology for both new and existing products.

3.2.4.2. **In particular, circumstances that reduce the risk of product or service are:**

- financial products or services that provide appropriately defined and limited services for specific customer groups in order to increase the availability of financial services;
- products that control the risk of money laundering and terrorist financing by other factors, such as monetary limits, in addition to those described in clauses 4.5.6.1 to 4.5.6.3 of the Guideline, or measures to increase transparency;
- basic payment services related to the payment account.

### 3.3. Specifying the customer's risk profile

3.3.1. **Low** risk level:

- 3.3.1.1. The customer's risk level is generally considered low if there is no risk factor of impact in any major risk category and there is at least one circumstance lowering the risk and it can therefore be claimed that the customer and its operations demonstrate elements that do not differ from those of an ordinary and transparent person; thereby there is no reason to suspect that the customer's operations may increase the probability of money laundering and terrorist financing.
- 3.3.1.2. In a situation where the application of the required measures of customer due diligence arises from legislation and information about the customer and its beneficial owner is publicly available, where the operations and transactions of the person are in line with its day-to-day economic activities and do not differ from the payment conventions and conduct of other similar customers or where the transaction is subject to quantitative or other absolute restrictions, the obligated person may deem the customer's estimated money laundering or terrorist financing risk to be lower.
- 3.3.1.3. In a situation where at least one risk category can be qualified as high, the risk level of money laundering or terrorist financing cannot usually be low. Equally, a low risk does not necessarily mean that the customer's operations cannot be associated with money laundering or terrorist financing at all.
- 3.3.1.4. If the risk resulting from a business relationship, a customer or transaction is low due to risk factors established with respect to the party to the transaction or the customer and the other conditions set out in clause 4.5 of the Guideline have been fulfilled, the employees of the financial service provider may apply simplified due diligence measures, but may not omit the customer due diligence measures entirely. Upon application of customer due diligence measures by way of the simplified procedure, the obligated person may determine the scope of application of the customer due diligence measures.
- 3.3.2. **High risk level:**
  - 3.3.2.1. The risk level of a customer is generally high when, in assessing the risk categories as a complex suspicion arises that the customer's activity is not normal or non-transparent, i.e., there is at least one of the circumstances mentioned in the higher risk category, which can be expected to be high or significantly increased in terms of money laundering and terrorist financing. The customer's risk level is high even if it is required by some risk factor (e.g., subject to international sanctions). In this case, high risk does not necessarily mean that the customer is engaged in money laundering or terrorist financing.
  - 3.3.2.2. The risk level is always considered high for a customer who has a residence or seat in a high risk third country or territory where no adequate measures to prevent money laundering and terrorist financing have been taken or if that state or territory does not cooperate internationally in the field of preventing money laundering and terrorist financing or is a territory with low tax rate.
  - 3.3.2.3. The risk level is always considered high when the circumstances of the transaction indicate that money laundering and terrorist financing, or its association with money laundering and terrorist financing, are likely to occur, including complex, high value and unusual transactions that do not have a reasonable economic purpose.
  - 3.3.2.4. If the employee of the Financial Service Provider assesses that the risk level of a customer or a participant in a transaction is high, the employee must apply customer due diligence in an enhanced manner as compared to the normal procedure to adequately manage the risks involved. In doing so, customer due diligence must be applied in an enhanced manner in accordance with the provisions of clause 4.6 of the Guideline.
  - 3.3.2.5. Transaction with low risk are transactions that do not refer to any of the risk-enhancing circumstances described in clause 3.2 and which are allowed to apply simplified customer due diligence measures in accordance as set out in clause 4.5.

- 3.3.2.6. High-risk transactions are transactions that clearly refer to one or more of the risk-enhancing circumstances provided in clause 3.2 and which are subject to enhanced customer due diligence measures as set out in clause 4.6.
- 3.3.2.7. The person in charge must record, update and assign the risk level, and make that information available to the competent authorities as appropriate.

#### **3.4. Identification of risks associated with new and existing technologies and services and products**

- 3.4.1. Before offering a new financial service or product, new or non-traditional sales channels to customers, or the introduction of new or emerging technologies, the management board of the Financial Service Provider, in cooperation with the Contact Person, assesses the risks of money laundering and terrorist financing involved.
- 3.4.2. For risk assessment, the management board of the Financial Service Provider, together with the Contact Person and, if necessary, other employees, maps the risks associated with each new product, service, technology or sales channel.
- 3.4.3. In assessing risks, both actual and potential risks are assessed and, if necessary, additional information on risks and their hedging measures is collected.
- 3.4.4. After mapping risks, the management board of the Financial Service Provider assesses the likelihood of the realization of risks and the level of risk, with particular emphasis on risk-enhancing and mitigating circumstances.
- 3.4.5. After assessing the risks and their effects, the Financial Service Provider assesses which of the most appropriate countermeasures to hedge the specific risks to the level of risk of the Financial Service Provider and, if necessary, arranges the implementation of countermeasures.
- 3.4.6. The Financial Service Provider assesses whether the application of countermeasures can lead to the risk of money laundering and terrorist financing associated with new financial services or products, new or non-traditional sales channels or new or emerging technologies in such a way as to meet the risk of a Financial Service Provider.
- 3.4.7. The provision of a new financial service or product, new or non-traditional sales channels to customers, or the introduction of new or emerging technologies can only be started if the risks of money laundering and terrorist financing are in accordance with the risk of the Financial Services Provider or can be brought about by the use of countermeasures to an acceptable level.
- 3.4.8. The management board of the Financial Service Provider records the results of a risk assessment which at least can be reproduced in writing.

## **4. Procedures for applying customer due diligence**

### **4.1. Applicable customer due diligence measures**

- 4.1.1. In providing the financial service the employees of the Financial Service Provider shall implement the following measures of diligence specified in § 20 of the AML/CFT Act:
  - 4.1.1.1. Identification of the customer or the participant in the transaction on the basis of the documents and information provided by him (see clause 4.3) and verification of the information provided on the basis of information obtained from a reliable and independent source, i.e. through the tools of e-identification and e-transaction trust services;
  - 4.1.1.2. Identification and verification of the representative of the natural or legal person;
  - 4.1.1.3. Identification of the beneficial owner and application of measures for verification of its identity to the extent that enables the Financial Services Provider to be sure that it knows who is the beneficial owner and understands the customer's ownership and control structure;
  - 4.1.1.4. Understanding of the business relationship or transaction and, where appropriate, obtaining additional information, specifying, inter alia, the customer's permanent place of business, place of business or residence, professional or field of activity, major trading partners, payment practices, in the case of a legal person, also experience;
  - 4.1.1.5. Obtaining information on the circumstance whether a person is a politically exposed person, member of its family or a person closely associated with it;
  - 4.1.1.6. Continuous monitoring of the business relationship;
  - 4.1.1.7. Collecting information on the origin of the customer's wealth, where appropriate.
- 4.1.2. The employee in charge of the Financial Service Provider applies the customer due diligence specified in clauses 4.1.1.1 to 4.1.1.5, as a minimum:
  - 4.1.2.1. In establishing a business relationship;
  - 4.1.2.2. In the event of suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or limitation referred to in law;
  - 4.1.2.3. In the event of doubt as to the adequacy or accuracy of the documents or data previously collected in the course of identification and verification of submitted information, or the updating of relevant data.
- 4.1.3. The financial service provider applies all customer due diligence set out in clauses 4.1.1.1 to 4.1.1.6 to the customer, but determines their scope and precise application and the need for applying the provisions of clause 4.1.1.7 on the basis of risks of money laundering or terrorist financing, previously assessed or specific to the business relationship or person.

### **4.2. Basic principles of customer due diligence**

#### **4.2.1. "Know your customer" principle**

- 4.2.1.1. Identifying the relevant information and data about the customer, including, in addition to the identification, the identification of the customer's activity profile, the purpose of its activity, the beneficial owner and, if applicable, the sources and origin used in the transaction, enabling the Financial Service Provider to assess whether the transactions performed by the customer correspond to its core field of activity and/or decide whether it is a normal or suspicious or unusual transaction.
- 4.2.1.2. An employee of the Financial Service Provider chooses the appropriate scope for applying the "Know Your Customer" principle, according to the principle of risk-based approach, to a particular business relationship or the risk level of the transaction.

#### **4.2.2. Principle of reasonableness**

- 4.2.2.1. In assessing customer due diligence of the Financial Service Provider, the principle of reasonableness is taken into account. For adequate application of due diligence by the Financial Services Provider, established in § 20 (1) of the AML/CFT Act, and regulated by this Guideline, the employee of Financial Services Provider responsible for the application of customer due diligence measures must be convinced that it has sufficiently applied the customer due diligence obligation. The principle of reasonableness is taken into account when considering the internal conviction, which, in accordance with the Law of Obligations Act, is general reasonableness by persons acting in good faith in the same situation. In assessing reasonableness, the purpose of the transaction, the habits and practices of the respective field of activity or profession as well as other circumstances are taken into account.

#### **4.3. Application of customer diligence when creating a business relationship**

##### **4.3.1. Purpose**

In addition to identification, the purpose of applying customer due diligence is also to determine the risk level of a customer in accordance with clause 3.2 of the Guideline.

##### **4.3.2. Identification of a natural person in establishing a business relationship**

###### **4.3.2.1. General requirements**

- 4.3.2.1.1. The Financial Service Provider shall identify the customer and, where appropriate, its representative, and keep the following data about the person and, where relevant, its representative:
- 4.3.2.1.1.1. name;
  - 4.3.2.1.1.2. personal identification code or, if not available, date and place of birth;
  - 4.3.2.1.1.3. place of residence or seat;
  - 4.3.2.1.1.4. information about the identification and verification of the right of representation and its scope, and if the right of representation does not arise from the law, the name of the document which is the basis for the right of representation, the date of issue and the issuer's name;
  - 4.3.2.1.1.5. activity profile;
  - 4.3.2.1.1.6. profession and field of activity;
  - 4.3.2.1.1.7. purpose and nature of creating a business relationship;
  - 4.3.2.1.1.8. beneficial owner if this is necessary in accordance with clause 4.3.2.7 of the Guideline.
- 4.3.2.1.2. Identification and verification of a natural person's identity is carried out on the basis of an identity document. Identification and verification are performed by the employees of the Financial Service Provider who are in direct contact with the customer.
- 4.3.2.1.3. The employee in charge records the person's place of residence and the profession or field of activity on the basis of its testimony.

###### **4.3.2.2. Documents used for identification:**

- 4.3.2.2.1. identity card;
- 4.3.2.2.2. digital identity card;
- 4.3.2.2.3. residence card;
- 4.3.2.2.4. passport of Estonian citizen;
- 4.3.2.2.5. diplomatic passport;
- 4.3.2.2.6. seaman's service book;
- 4.3.2.2.7. foreigner's passport;
- 4.3.2.2.8. temporary travel document;

- 4.3.2.2.9. refugee's travel document;
- 4.3.2.2.10. maritime certificate;
- 4.3.2.2.11. return certificate;
- 4.3.2.2.12. return authorization;
- 4.3.2.2.13. a valid travel document issued abroad;
- 4.3.2.2.14. driving license with a user name, photo or facial image, signature or signature image and date of birth or personal identification code.
- 4.3.2.3. The employee in charge of the Financial Service Provider evaluates the submitted document's:
  - 4.3.2.3.1. Expiry date;
  - 4.3.2.3.2. External similarity of the person and the suitability of the age with the appearance of the person depicted in the document;
  - 4.3.2.3.3. Personal identification code for gender and age;
  - 4.3.2.3.4. In the case of information contained in the codes given to foreign natural persons regarding the authenticity or identity of the document, a foreign mission or other competent authority is consulted.
- 4.3.2.4. An employee shall make a copy of the personal data and photographic pages provided on the submitted document and shall record other information received on the person in the Financial Services Provider's information system.
- 4.3.2.5. An employee does not make a copy of the document if the Financial Services Provider has entered into a data exchange contract with the Police and Border Guard Board on the basis of which the Financial Services Provider can make inquiries into the Identity Documents Database.
- 4.3.2.6. **Politically exposed person**
  - 4.3.2.6.1. In addition to the identification, the employee of the Financial Service Provider, in applying customer due diligence also establishes whether the person is a politically exposed person or not.
  - 4.3.2.6.2. In particular, the fact is whether the person is a politically exposed person based on the testimony and assurances given by the customer. If the employee suspects that, despite the customer's claims, the customer is a politically exposed person, the employee shall then make initial checks using Internet search engines or relevant databases. If the suspicion is permanent, the employee shall contact to its superior who, if necessary, shall consult the Contact Person or the management board of the Financial Service Provider to obtain further guidance.
  - 4.3.2.6.3. The employee of the Financial Service Provider shall also identify close associates of the politically exposed person, and family members if there is reason to believe that such an association exists.
- 4.3.2.7. **Identification of the beneficial owner**
  - 4.3.2.7.1. Identification of the beneficial owner of a natural person in the event of doubt occurring when a worker feels that a natural person has been requested, attracted, threatened, abandoned or otherwise biased towards establishing a business relationship or making a transaction. In this case, the person who exercises control over the natural is considered to be the beneficial owner of the natural person.
- 4.3.2.8. **Verification of documents and data**
  - 4.3.2.8.1. The employee of the Financial Service Provider verifies the data and references provided to identify the person through reliable and

independent sources of information, including public registers and public authorities.

- 4.3.2.8.2. The information is regularly verified and the employee in charge of the Financial Services Authority is responsible for this.

#### **4.3.3. Identification of a legal person in establishing a business relationship**

- 4.3.3.1. In identifying a legal entity, the following must be determined:

- 4.3.3.1.1. Business name;
- 4.3.3.1.2. Register code;
- 4.3.3.1.3. Location and place of business;
- 4.3.3.1.4. Information about the legal form and legal capacity of the person;
- 4.3.3.1.5. Names of the members of the management board and their powers in representing the legal person;
- 4.3.3.1.6. Telecommunications data;
- 4.3.3.1.7. Data of the representatives, while complying with the provisions of clause 4.3.4 of the Guideline;
- 4.3.3.1.8. Existence of politically exposed persons;
- 4.3.3.1.9. Actual beneficial owners, in accordance with the provisions of clause 4.3.3.4 below

- 4.3.3.2. Legal entity is identified on the basis of a registry card, registration certificate or equivalent document. If the Financial Service Provider has access to the data of the Commercial Register, non-profit associations and foundations register or foreign relevant registries through the computer network, this customer does not need to submit the registration card to the Financial Service Provider.

- 4.3.3.3. Employee in charge shall copy the information contained in the personal data of the representatives of the persons and record the data obtained from the legal entity in the information system of the Financial Service Provider, in particular:

- 4.3.3.3.1. Head of the legal person, in the case of foreign companies, the names of the members of the management board or other body replacing it, and their representation powers;
- 4.3.3.3.2. Main field of activity of the legal person;
- 4.3.3.3.3. Actual beneficial owners of the legal entity (including data on the ownership of the group and the ownership structure of the group).

#### **4.3.3.4. Identification of the beneficial owner**

- 4.3.3.4.1. If no natural person's participation or detectable control rate does not exceed 25%, information about shareholders, shareholders, partners or other persons having control over the legal person or other significant influence is required.
- 4.3.3.4.2. If the documents presented in the course of identification does not directly indicate who is the beneficial owner of the legal entity, the corresponding data shall be recorded on the basis of testimony of the representative of the legal person or its own written document.
- 4.3.3.4.3. Correctness of the data provided on the basis of statements or personal written documents is checked for reasonable measures, including the submission of inquiries to the relevant registers, the annual report of the legal person or the submission of an appropriate document. Upon acceptance of the testimony or self-written document, the employee informs the customer of the liability that comes with the submission of misleading or false information.

#### **4.3.4. Identification and verification of the right of representation**



- 4.3.4.1. The employee in charge must determine whether the person acts on his own behalf or on behalf of another (natural or legal) person. If a person acts on behalf of another person, the employee must also explain the person on whose behalf the transactions are carried out.
- 4.3.4.2. The employee must determine the basis, scope and expiry date of the representative's right of representation.
- 4.3.4.3. For authorized and statutory representatives, it must be made clear whether the representative is familiar with the representative. In this case, it is checked whether the representative knows:
  - 4.3.4.3.1. The content and purpose of the statements of the person represented by it;
  - 4.3.4.3.2. Economic and professional activities represented;
  - 4.3.4.3.3. Purpose of the transactions;
  - 4.3.4.3.4. Person's business partners;
  - 4.3.4.3.5. Source and origin of the funds used in the transaction;
  - 4.3.4.3.6. Ownership of the legal entity.
- 4.3.4.4. The representative confirms with his signature that it is aware and convinced of the source and legal origin of the funds used in the transaction being represented.

#### **4.4. Procedure for updating the data/documents used to identify the identity**

- 4.4.1. The employee of the financial service provider updates the data obtained from the identification and verification of the identity at least twice a year, at the level of the enhanced risk every three (3) months.
- 4.4.2. To update, the Financial Services Provider uses the following methods and measures:
  - 4.4.2.1. Verifies data in public databases and registers;
  - 4.4.2.2. When the document expires, it contacts the customer and requests an updated version of the document.

#### **4.5. Simplified application of diligence measures**

- 4.5.1. An employee of the Financial Service Provider applies the customer due diligence measures specified in the Guideline in a simplified manner in the case of a low risk of money laundering or terrorist financing if the customer's risk profile is low and the risk assessment made by the Financial Services Provider has established that, in such circumstances, the situation is lower than the situation of money laundering or terrorist financing.
- 4.5.2. Before applying the customer due diligence measures, the Financial Service Provider determines that the business relationship, transaction or transaction is less risky and may set a lower risk standard than such a transaction, transaction or customer. In particular, prior to applying the customer due diligence measures, the employee of the Financial Services Authority assesses the occurrence of the minor risk factors specified in clauses 3.2.2.1 and 3.2.3.2 of the Guideline and apply them as separate grounds (i.e., each occurrence of the circumstances allows the customer to apply diligence measures in a simplified manner).
- 4.5.3. The Financial Service Provider applies customer due diligence measures in a simplified manner only to the extent that adequate monitoring of transactions and business relationships is ensured in order to detect abnormal transactions and allow for reporting of suspicious transactions.
- 4.5.4. In the simplified application of the diligence measures set out in clauses 4.1.1.1 and 4.1.1.2 of the Guideline, the identity of the customer and its representative can be checked from the information obtained from a reliable and independent source during the creation of a

business relationship if this is necessary in order not to disturb the normal course of business.

- 4.5.5. In the application of clauses 4.1.1.3 - 4.1.1.5 of the Guideline, when applying the simplified procedure, the financial service may be chosen in the extent of the obligation and the need for verification of the source and data of the reliable and independent source of data used for this purpose.
- 4.5.6. The customer due diligence measures provided for in clause 4.1.1.6 of the Guideline may be applied in a simplified manner if a lower risk is identified and if at least the following conditions are met:
  - 4.5.6.1. A contract is concluded in the form of a written, electronic or in a written reproducible format with the customer;
  - 4.5.6.2. The Financial Service Provider receives payments in the framework of a business relationship only through an account located in a credit institution incorporated in the commercial register of Estonia or a branch of a foreign credit institution or a credit institution established or operating in a Contracting State of the European Economic Area or in an equivalent country;
  - 4.5.6.3. The total value of incoming or outgoing payments in business relationships does not exceed EUR 15,000 per year.
- 4.5.7. In the case of transactions, the criterion of low risk may be the fact that the benefits of the transaction are not realized as a third party's benefit, except for death, incapacity for work, predetermined high age or similar event.
- 4.5.8. The customer due diligence measures do not apply to the simplified procedure if the employee has suspected money laundering or terrorist financing.

#### **4.6. Enforcement of the customer due diligence measures**

- 4.6.1. The Financial Service Provider applies the customer due diligence measures in an enhanced manner in order to properly manage and mitigate the risk of money laundering and terrorist financing above the usual standard.
- 4.6.2. The customer due diligence measures are applied in an enhanced manner whenever:
  - 4.6.2.1. In the course of identification or verification of the information provided by the customer, doubts arise as to the truth of the submitted data or the authenticity of the documents or the identification of the beneficial owner(s);
  - 4.6.2.2. a customer or a participant in a transaction is a politically exposed person (except for a person with Estonian national background), its family member or a close associate;
  - 4.6.2.3. The customer or a participant in a transaction is from a high-risk third country, its place of residence or seat or the seat of the payee's payment service provider is located in a high-risk third country;
  - 4.6.2.4. The customer or transaction is from such country or territory or its place of residence or location, or the payment service provider of the payee is located in a country or territory where reliable sources, such as peer reviews, reports or published follow-up reports, do not provide effective systems for the prevention of money laundering and terrorist financing, which is in line with the recommendations of the Money Laundering Advice Council, or considered a low tax area.
  - 4.6.2.5. The risk assessment prepared by the Financial Service Provider on the basis of clause 3.1 of this Guideline has established that in such circumstances, the situation is greater than the usual money laundering or terrorist financing situation.
- 4.6.3. The customer due diligence measures are applied in an enhanced manner even if, based on the risk profile of the customer and the risk assessment, it has been established that its field of business or profession, sector or circumstances, the situation is greater than the normal risk situation of money laundering or terrorist financing.

- 4.6.4. Prior to applying the customer due diligence measures, the employee of the Financial Service Provider determines that the risk of the business relationship, transaction, or operation is enhanced and that a higher risk profile can be set for such a transaction, transaction or customer. In particular, prior to the application of the customer due diligence measures, the Financial Service Provider shall, in addition to the application of the customer due diligence measures, assess the occurrence of the circumstances mentioned in clauses 3.2.2.1., 3.2.4.1. and 3.2.3.1 of the Guideline and the abovementioned higher risk factors, and apply them as separate grounds (i.e., each factor indicated requires enhanced application of customer due diligence measures for the customer) When applied enhanced customer due diligence measures, at least one of the following additional customer due diligence measures is followed:
- 4.6.4.1. Identification and verification of the submitted information on the basis of supporting documents, data or information derived from a reliable and independent source or from a credit institution incorporated in the commercial register in Estonia or a branch of a foreign credit institution or a credit institution that is registered or has its place of business in a Contracting State of the European Economic Area or in a country subject to equivalent requirements as prescribed by law;
- 4.6.4.2. Application of additional measures to verify the authenticity of the documents submitted and the accuracy of the information contained therein, including requiring their notarial or official confirmation or confirmation of the accuracy of the data by the credit institution referred to in the previous paragraph which issued the document;
- 4.6.4.3. Collection of additional information on the purpose and nature of the business relationship or transaction and verifying the information provided on the basis of supporting documents, data or information originating from a reliable and independent source;
- 4.6.4.4. Collection of additional information and documents on the actual execution of transactions and identifying the source and origin of the funds used in the transaction in order to rule out the likelihood of transactions;
- 4.6.4.5. Making a first payment on a transaction through an account opened in the name of the person participating in the transaction or in the name of the customer in a credit institution registered or having its registered office in a Contracting State of the European Economic Area or in a country where the requirements equivalent to those provided for in the Act are in force;
- 4.6.4.6. Customer due diligence measures applied to the customer or its representative while staying at the same place.
- 4.6.5. If the customer due diligence measures are applied, the Financial Service Provider shall more frequently apply the monitoring of the business relationship and re-evaluate the risk profile of the client no later than six months after the establishment of the business relationship.
- 4.6.6. **Additional due diligence for transactions involving persons with a high-risk third country**
- 4.6.6.1. If a Financial Service Provider, in the course of its business or business transaction or through a customer, is in contact with a high-risk third country, it shall apply the following customer due diligence measures:
- 4.6.6.1.1. Obtaining additional information about the customer and its beneficial owner;
- 4.6.6.1.2. Obtaining additional information about the planned content of the business;
- 4.6.6.1.3. Obtaining information about the financial resources of the customer and its beneficial owner and the source of wealth;

- 4.6.6.1.4. Obtaining information about the causes of planned or executed transactions;
  - 4.6.6.1.5. Obtaining a permission from the management board to establish or continue the business relationship;
  - 4.6.6.1.6. Improving the monitoring of the business relationship by increasing the number and density of the control measures applied and selecting transaction characteristics to be further verified;
  - 4.6.6.1.7. Requiring payment only from an account in the name of a customer from a Contracting State of the European Economic Area or from a third-country credit institution applying equivalents.
- 4.6.6.2. An employee of a Financial Service Provider shall notify its immediate superior as soon as a person operating in a high-risk third country wishes to become a customer of the Financial Service Provider who then notifies the Contact Person who decides on the application of the following measures and their extent.
- 4.6.7. **Creating business relationships with a politically exposed person**
- 4.6.7.1. For politically exposed persons, the following follow-up measures are applied:
- 4.6.7.1.1. Requesting additional information from the customer in order to identify sources of assets and funds used in business relationships or transactions;
  - 4.6.7.1.2. Checking the data or making inquiries into the databases of state authorities of the respective country and the search and verification of data on the Internet;
  - 4.6.7.1.3. Making inquiries or verifying data from websites of the relevant supervisory authorities or institutions of the customer's or person's home country.
- 4.6.7.2. The establishment of a business relationship with a politically exposed person shall be decided by the management board of the Financial Service Provider.
- 4.6.7.3. The employee verifying the data will inform the management when the customer or the beneficial owner proves later or becomes a politically exposed person.
- 4.6.7.4. Regular enhanced checks are implemented in business relationships with a politically exposed person. Regular enhanced checks will also be implemented after the person has ceased to act as a politically exposed person if, due to the principle of risk-based approach to this person, he or she continues to have enhanced risk.
- 4.6.7.5. Regarding a politically exposed person, additional vigilance measures shall be taken at least 12 months after the politically exposed person has ceased to fulfill significant public duties.
- 4.6.7.6. Financial Service Provider may waive the additional customer due diligence measures specified in clause 4.6.7 of this Guidelien if the customer is a politically exposed person in the Republic of Estonia and there are no other circumstances indicating a higher risk than usual.
- 4.6.8. **The purpose and nature of the business relationship and the transaction, further monitoring**
- 4.6.8.1. The employee in charge determines the business relationship and the purpose and nature of the transaction on the basis of the following information:
- 4.6.8.1.1. Confirmations issued by the customer in establishing a business relationship or performing a transaction;
  - 4.6.8.1.2. Information obtained from the customer's business profile and field of activity.
- 4.6.9. **Application of the "Know Your Customer" principle**
- 4.6.9.1. **Effective identification of a person's customer profile**

In order to effectively and promptly determine whether a person is (i) a politically exposed person, (ii) a person whose place of residence is in a country where adequate measures to prevent money laundering and terrorist financing have not been adopted, (iii) whose activities have previously been suspected of being involved in money laundering or terrorist financing; (iv) a person who is subject to international sanctions; or (v) a person using a transaction through telecommunication, the responsible employee shall use appropriate websites and databases. The availability and use of the necessary databases (including access and necessary training) is the responsibility of the member of the management board responsible for establishing and controlling the prevention of money laundering.

**4.6.9.2. For the application of the "Know Your Customer" principle, the employee in charge must**

- Implement measures to identify the area of activity and profile of the customer, incl
- Request data from a customer when creating a business relationship or making a transaction;
- Control of public databases and registers (e.g., MTR)
- Monitor, analyze and distinguish between transactions performed by a customer with a Financial Service Provider and financial institutions belonging to the same group as the Financial Service Provider;
- If the in employee in charge has a suspicion of money laundering or terrorist financing related to a low-risk transaction, it must apply enhanced customer due diligence measures in accordance with the provisions of clause 3.5 of the Guideline.

**4.6.9.3. The monitoring of the business relationship must include at least the following**

- Checking transactions in business relationships to ensure that transactions are in accordance with the Financial Service Provider's knowledge of the customer, its activities and risk profile;
- Regular updating of the relevant documents, data or information collected during the application of customer due diligence measures;
- Identification of source and source of funds used in the transaction;
- Increased focus on business transactions, customer activities and circumstances that point to criminal activities, money laundering or terrorist financing, or which are likely to be linked to money laundering or terrorist financing, including complex, high value and unusual transactions and transaction patterns that do not have a reasonable or visible economic impact or for a legitimate purpose or which is not specific to a particular business specification, including the nature, causes and background of these transactions, as well as other information for understanding the content of the transactions;
- paying more attention to a business relationship or transaction if the customer comes from a high-risk country or a country or territory specified in clause 3.2.3.1 of the Guideline, or is the national of that country or its place of residence, or the payment service provider of the payee is located in that country or territory.

**4.6.9.4. When monitoring a business relationship, employees must**

- Monitor and keep in mind the list of money laundering suspicious transactions issued by the Financial Intelligence Unit;
- Verify the customer's transactions with frequency that corresponds to the risk level of the customer, bearing in mind that in the case of low-risk customers, the controls should be carried out at least once a year and for high-risk customers, verification should be carried out for each transaction;

- inform the Contact Person of any suspicion of money laundering or terrorist financing transactions;
- To change the customer's risk level as a transaction with a low-risk client

#### **4.7. Refusal to execute a transaction and termination of business relationship**

- 4.7.1. In a situation where an employee of the Financial Service Provider, based on the documents collected in the course of the customer due diligence measures of the business relationship, suspects money laundering or terrorist financing or its attempt, or if the employee suspects that the person is subject to an international sanction, the establishment of a business relationship is prohibited.
- 4.7.2. The Financial Service Provider does not establish a business relationship (the creation of a business relationship and the making of a transaction is prohibited) if the person or customer involved in the transaction or official action, despite the relevant request, fails to submit the documents and relevant information required to comply with the customer due diligence measures specified in clauses 4.1.1.1 to 4.1.1.6 of the Guideline and on the basis of the documents submitted, the employee suspects that money laundering or terrorist financing may be involved.
  - 4.7.2.1. The Financial Service Provider has the right to refuse to execute the transaction if the person or customer involved in the transaction, despite the relevant request, fails to submit the documents and relevant information or documents certifying the legal origin of the object of the transaction to identify the circumstances specified in clauses 4.1.1.1 to 4.1.1.6 of the Guideline or if, on the basis of the data and documents submitted, the obligated person has suspicion that money laundering or terrorist financing may be involved.
  - 4.7.2.2. If, in spite of the request, the person or customer participating in an economic activity does not submit the documents or relevant information required to comply with the obligations set out in clauses 4.1.1.1 to 4.1.1.6 of the Guideline, it is regarded as a significant breach of contract and the Financial Service Provider has the obligation to prematurely terminate the duration contract that is the basis for the business relationship without giving prior notice.
- 4.7.3. It is prohibited to establish a business relationship or make a transaction with a person whose capital consists of bearer shares or other bearer securities.
- 4.7.4. In case of refusal to make a transaction or establish a business relationship, and in case of an premature cancellation of the duration contract, which is the basis for the business relationship, the responsible employee must register and keep a statement on the more precise circumstances of the refusal or cancellation, as well the other information on which the information obligation is based, according to the procedure for collecting and storing data specified in this Guideline (in accordance with clause 6 of this Guideline).
- 4.7.5. Establishing a business relationship or making a transaction in the cases provided for in clause 4.7 of this Guideline is permitted if the Financial Service Provider has notified the Financial Intelligence Unit pursuant to the procedure provided for in clause 7 of the Guideline and has received a specific instruction from the Financial Intelligence Unit about the business relationship, establishment of a business relationship or execution of a transaction.
- 4.7.6. If the Financial Service Provider refuses to establish a business relationship or making a transaction or prematurely terminates the duration contract that is the basis for the business relationship on the bases provided for in clause 4.7 of the Guideline and the person has transferred funds to the Financial Service Provider's account, the Financial Service Provider shall transfer the transferred funds only to the customer account opened in the credit institution entered in the commercial register in Estonia or a branch of a foreign credit institution or a credit institution which is incorporated or whose place of business is in a

Contracting State of the European Economic Area or in a country subject to equivalent requirements. The property may be transferred to an account other than the customer's account only if it is notified to the Financial Intelligence Unit at least seven days in advance and the Financial Intelligence Unit does not issue a different order.

4.7.7. The provisions of clause 4.7 may not be applied only on the grounds provided by law.

#### **4.8. Subjects of International sanctions**

4.8.1. The subject of an international sanction is: a natural or legal person, an authority, a partnership or any other entity directly identified in an instrument imposing or implementing an international sanction and subject to the measures provided for by an instrument imposing an international sanction.

4.8.2. The person responsible for the implementation of the international financial sanctions is the Contact Person appointed by the management board. The management or any other person authorized by the Financial Service Provider shall forward the contact details of the Contact Person to the Financial Intelligence Unit.

4.8.3. Upon the entry into force of a law establishing or enforcing international financial sanctions, employees shall take measures to fulfil their obligations and demonstrate the necessary diligence in order to ensure the achievement of the objective of international financial sanctions and to prevent a sanction violation.

4.8.4. The responsible employee pays special attention to the activities and circumstances of a person who has a business relationship with the Financial Services Provider or performs a transaction or act, or plans the establishment of a business relationship or the making of a transaction or act which indicate that the person is subject to international financial sanctions.

4.8.5. If the responsible employee is suspicious or knows that a person who is engaged in a business relationship with the Financial Services Provider or a person acting in the transaction or operation, as well as the establishment of a business relationship or the person who proposes to carry out the transaction or operation is the subject of international financial sanctions, the employee shall immediately inform the Financial Intelligence Unit about the identification of a subject of the international financial sanction, its suspicion and measures taken.

4.8.6. If the person who has a business relationship with the creditor or performs a transaction or act as well as the person planning the establishment of a business relationship or planning a transaction or act refuses to provide additional information or it is not possible to determine whether the person is a subject of international financial sanctions, the person in charge shall refuse to perform the transaction or act, and shall inform the Contact Person who shall take the measures provided for in the legislation establishing or implementing the international financial sanctions and promptly inform the Financial Intelligence Unit of its suspicion and action.

4.8.7. The Contact Person is obliged to regularly monitor the website of the Financial Intelligence Unit and take immediate steps to ensure that the international financial sanctions target is achieved and to prevent the violation of the international financial sanctions provided for in the legislation establishing or implementing the international financial sanctions.

4.8.8. Upon the entry into force, amendment, revocation or expiration of a legal act imposing or applying international financial sanctions, the Contact Person or the person authorized by the Contact Person shall immediately verify whether the person who is engaged in the business relationship with the Financial Service Provider or the person acting in the transaction or act as well as person who plans to establish a business relationship or plans to engage in the transaction or act is an international subject to financial sanctions against whom a financial sanction is imposed, amended or terminated.

4.8.9. The form of the notice to the Financial Intelligence Unit has been established by the Minister of Internal Affairs Regulation No. 51 from 4.10.2010 "Form for the notice to the Financial

Intelligence Unit and instructions for its completion.” The use of the form prescribed in the Regulation is mandatory.

- 4.8.10. The employee in charge shall pay attention to the factors that distort personal data. Factors that distort personal data are the following errors or differences in the translation, handling or processing of personal data and names:
- 4.8.10.1. Transcription of foreign names, including: romanization differences between Russian and Scandinavian names;
  - 4.8.10.2. Different order in the words of a name or a name composed of several Word
  - 4.8.10.3. Replacement of letters with diacritics (letters with umlauts or without punctuation) with other letters or their (partial) omission;
  - 4.8.10.4. Replacement of double letters and foreign letters with other letters or their (partial) omission:
    - Replacement of double letters with single letters (and vice versa);
    - Replacement of the letters F, Š, Z, Z, C ... with other letters or letter combinations;
    - Replacement of alphabetic characters W, Q, X, Y ... with other letters.
  - 4.8.10.5. Use of abbreviations;
  - 4.8.10.6. Typing the numbers in the text, for example 2 FAST 4 YOU or TWO FAST FOUR/FOR/YOU;
  - 4.8.10.7. Use/non-use of suffices and prefixes;
  - 4.8.10.8. Other factors:
  - 4.8.10.9. lapsus calami (mistakes due to human error);
  - 4.8.10.10. Replacement of hard and soft sounds;;
  - 4.8.10.11. Occurrence of a name or part thereof in another name or part thereof.
- 4.8.11. The contact person appointed by the management board collects and maintains the following information for a period of five years:
- 4.8.11.1. Time of inspection;
  - 4.8.11.2. Name of the inspector;
  - 4.8.11.3. Results of inspection;
  - 4.8.11.4. Measures taken.



## **5. Transfer of business**

### **5.1. Conditions for the transfer of business**

- 5.1.1. The Financial Service Provider may assign the obligation to identify a person to a third party who is:
  - 5.1.1.1. Person obligated within the meaning of the act;
  - 5.1.1.2. An organization, association or society, the members of which are persons obligated within the meaning of the Act; or
  - 5.1.1.3. another person who applies the diligence measures and data retention requirements set out in the Act and who is, or is prepared to be, in a Contracting State in the European Economic Area, in the context of the prevention or control of money laundering.
- 5.1.2. The Financial Service Provider will not transfer the activities to a person established in a third-country high risk.
- 5.1.3. Activities will be transferred only to third parties who have the necessary knowledge and skills or preconditions for acquiring their knowledge and skills and who are able to fulfil the obligations prescribed by law and the Guideline. The Financial Services Provider shall notify a third person of any laws, other legislation issued pursuant to laws, relevant requirements of the Financial Supervision Authority and the RAB guidelines and the Guideline, and reserves the right to verify compliance with the requirements for the performance of the transfer. The financial Service Provider reserves the right to cancel the contract with a third party in the performance of his duties in the event of defects.
- 5.1.4. If necessary, the Financial Services Provider provides training to third parties (and its employees) on money laundering and terrorist financing that is carried out by a responsible employee or other relevant field expert appointed by the Financial Services Provider. The Financial Service Provider may allow a third party (and its employees) to participate in training of the employees of the Financial Services Provider, if the parties agree. If the need for third-party training in the field of money laundering and terrorist financing prevention is low, the Financial Services Provider must explain to the third party at least the requirements specified in the Instructions, and in the event of changes in the Guideline, in the case of changes in international practice or legislation, inform the third person thereof.
- 5.1.5. Both the suitability of a third party and the need for training are assessed on the basis of its normal professional and business activities and the main duties of the third person or of its employees, education, and other circumstances that may indicate a person's lack of knowledge or ability to carry out activities carried out.

### **5.2. Contract for the transfer of business**

- 5.2.1. The Financial Service Provider shall continue to perform activities only in a manner that does not adversely affect the legitimate interests of itself or its customers, its activities and compliance with the obligations provided by law and this Guideline, as well as the exercise of state supervision over him. In doing so, the Financial Service Provider is guided in the transfer of the duties by at least the following conditions:
  - 5.2.1.1. The managers of the Financial Service Provider must not delegate their responsibility upon the transfer;
  - 5.2.1.2. The transfer must not adversely affect the interests of the customers of the Financial Service Provider and the relations with the customers and the obligations towards the customers may not change due to the transfer;
  - 5.2.1.3. The transfer must not be in conflict with the terms and conditions which the Financial Service Provider must fulfil in order to obtain authorization and to comply with the license;
  - 5.2.1.4. The transfer shall not invalidate or modify any other terms under which the Financial Service Provider has been authorized.

- 5.2.2. In order to transfer the business, the Financial Service Provider signs a written agreement ensuring that:
- 5.2.2.1. The transfer of business does not prevent the activities of the Financial Service Provider or the fulfilment of the obligations provided for in the Law or the Guideline;
  - 5.2.2.2. A third party meets all obligations of the Financial Service Provider that relate to the transfer of activities;
  - 5.2.2.3. The transfer of business does not prevent the supervision of the Financial Services Provider;
  - 5.2.2.4. It is possible for the Financial Intelligence Unit to supervise the person carrying out the transferred activity through the Financial Service Provider, including through an on-site inspection or other supervisory measure;
  - 5.2.2.5. The person performing the activity has the necessary knowledge and skills and the ability to comply with the requirements provided by the Act and the Guideline;
  - 5.2.2.6. The right of the Financial Service Provider to restrict the compliance with the requirements set forth in the Act and the Guideline without restriction;
  - 5.2.2.7. The storage of documents and data collected in order to meet the requirements of the Act and the Guideline, and at the request of the Financial Service Provider, the prompt transfer of documents or other relevant documents relating to the identification of the customer and his beneficial owner or submission to the competent authority.
- 5.2.3. In identifying a person, the third party immediately informs the Contact Person of suspicion of money laundering and terrorist financing who then informs RAB as provided for in this Guideline.

### **5.3. Obligations of third parties**

- 5.3.1. The third party is obliged to comply with the customer due diligence measures and data collection and storage requirements, which are also applied by the responsible employee of the Financial Services Provider, in fulfilling the delegated obligations.
- 5.3.2. This Guideline is applied by the third party to whom the activity is transferred, on the same basis as the employee in charge. The third party (or its employee) confirms the introduction to the Guideline by its signature.

### **5.4. Notification about the transfer of business**

- 5.4.1. The Financial Service Provider shall inform the Financial Intelligence Unit of the conclusion of the contract for the transfer of business at least 2 business days before the conclusion of the contract. In the notice, the Financial Services Provider shall indicate, inter alia, the extent of the transmitted activity. At the request of the RAB, the Financial Service Provider submits to the RAB a contract for the transfer of activities.

## **6. Procedure for collecting and storing data**

### **6.1. Storage of used data**

- 6.1.1. The employee in charge retains the data and documents used to identify the customer identified in clause 4.3 of the Guideline in such a way that their written reproduction has been at least as large as possible:
  - 6.1.1.1. The information specified in clauses 4.3.2.1.1 and 4.3.3.1 of the Guideline;
  - 6.1.1.2. Copy of the document used for identification;
  - 6.1.1.3. The method, time and place for the submission or updating of data and documents;
  - 6.1.1.4. Other data collected for identification purposes and an indication of whether the data was collected for establishing a business relationship, including account opening, or for the use of another service that does not require account opening;
  - 6.1.1.5. Information on the establishment of a business relationship or the refusal to execute a transaction or the circumstances of termination of a business relationship;
  - 6.1.1.6. On the initiative of the customer, the circumstances of waiving the performance of the transaction or establishment of a business relationship, if the waiver has been related to the application of customer due diligence measures;
  - 6.1.1.7. Name and job title of the employee who made the identification, verified or updated the data.
- 6.1.2. The data mentioned in clause 6.1.1.1 must be kept together with the name and title of the employee who updated the data and the facial image and signature image of the document user in a written reproducible format if, when establishing a business relationship, the customer is identified on the basis of a document for certifying a digital person issued in the Republic of Estonia without being present in the same place.

### **6.2. Registration of data**

- 6.2.1. For all transactions or act, the content of the transaction or act as well as the time or period of the transaction or act shall be recorded. In identifying a person and checking the information submitted, the corresponding act is recorded for the date or period of the inspection.
- 6.2.2. The following data is recorded for the transaction:
  - 6.2.2.1. The account number used by the customer is the name of the account holder and the bank where the corresponding account is open;
  - 6.2.2.2. Transaction currency;
  - 6.2.2.3. Date of entry of each entry and explanation of the entry.
- 6.2.3. The Financial Service Provider shall further record the following information:
  - 6.2.3.1. The circumstances of the refusal to establish a business relationship with the customer by a Financial Service Provider;
  - 6.2.3.2. The circumstances in which a business relationship with a customer is created or a transaction is cancelled, if the waiver is related to the application of diligence measures by the Financial Service Provider;
  - 6.2.3.3. All information collected, if customer due diligence measures cannot be applied with the help of IT tools;
  - 6.2.3.4. Circumstances for the termination of the business relationship due to the impossibility of applying due diligence measures;
  - 6.2.3.5. Circumstances related to suspicion of money laundering.

### **6.3. Data retention deadlines**

- 6.3.1. Information about the business relationship (i.e., the correspondence relating to the application of diligence measures, the documents collected during the monitoring of the

business relationship, and data on suspicious or unusual transactions or circumstances not notified to the Financial Intelligence Unit) shall be retained for at least five years from the termination of the business relationship.

- 6.3.2. Information about the transaction shall be kept for at least five years from the date of transaction.
- 6.3.3. Information about the fulfilment of the obligation to inform the Financial Intelligence Unit shall be kept for at least five years from the date of the obligation to notify.
- 6.3.4. The Financial Service Provider shall ensure the deletion of the data collected after the expiry of their retention period, unless a longer term of retention is required by law, other legislation or precept.

#### **6.4. Protection of personal data**

- 6.4.1. The data created during the establishment and in the course of the business relationship shall be used only for the fulfilment of the obligations provided for in this Guideline and shall not be used in other ways or for purposes not specified herein, except if the customer has given his consent to the use of the data for other purposes.
- 6.4.2. Prior to establishing a business relationship, the Financial Services Provider provides the potential customer with information about the processing of personal data. This information also provides general information on the Financial Service Provider's processing of personal data for the purposes of money laundering and terrorist financing.
- 6.4.3. The Financial Service Provider applies all the rules for the protection of personal data provided for in the Personal Data Protection Act in the application of the requirements arising from this Guideline.

## 7. Compliance with the notification procedure

- 7.1.** In a situation in which relations with the customer reveal unusual circumstances or where the employee of the Financial Services Provider suspects money laundering or terrorist financing, it must be immediately notified to the Contact Person designated by the management board of the Financial Service Provider who decides on whether to immediately forward the information to the Financial Intelligence Unit. The Contact Person must inform the Financial Intelligence Unit immediately, but not later than within two working days, of any suspicion of money laundering. Among others, the Financial Intelligence Unit must be informed if the person in charge has refused to establish a business relationship or to make a transaction, or terminates prematurely a business relationship due to the refusal to provide the necessary information for the application of due customer diligence measures or because of non-submission in spite of the request.
- 7.2.** In accordance with the procedure set out in clause 7.1, the Financial Intelligence Unit must also be notified of the following:
- 7.2.1. Establishing a business relationship, transaction or act or providing a service remains unfulfilled;
  - 7.2.2. The establishment of a business relationship or transaction is denied due to the impossibility of applying customer due diligence measures;
  - 7.2.3. The establishment of a business relationship or the performance of a transaction is refused due to the person's capital being comprised of bearer shares or other bearer securities;
  - 7.2.4. The customer does not submit, despite the relevant request, the documents and relevant information or evidence of the origin of the object of the transaction, or the document or the submitted data and documents, there is a suspicion that it may be money laundering or terrorist financing;
  - 7.2.5. Any transaction in which a financial liability of EUR 32,000 or equivalent in another currency is paid in cash regardless of whether the transaction is executed as a single payment or several interrelated payments for up to one year.
- 7.3.** An employee of the Financial Service Provider who meets the requirements for Contact Person in the law is appointed as Contact Person. The Contact Person is directly subordinated to the management board of the Financial Services Provider. The tasks of the Contact Person are:
- Arranging and analyzing the collection of information indicating abnormal or money laundering suspected transactions or terrorist financing in the activities of a Financial Service Provider;
  - Forwarding of information to the Financial Intelligence Unit in case of suspicion of money laundering or terrorist financing;
  - Quarterly submission of written reviews to the management board of the Financial Service Provider on the compliance with the Guideline;
  - Fulfilment of other obligations provided to the Contact Person by the Guidelines or by law.

The main conditions to be considered when analyzing suspicious and unusual transactions are as follows:

- Is there a suspicious circumstance in the operations, transactions or other circumstances?
- Is the Financial Service Provider convinced that it knows the customer to the extent necessary or is it in need of additional data collection?
- The Financial Service Provider must, in carrying out the transaction or transaction identification transaction of the customer or its representative, verify that it has complied with the prescribed procedures. Was all the information or data that was

provided incomplete, the data had to be asked or otherwise required to be specified?

- Find out if there have been repeated occurrences of suspicious operations and transactions.

- 7.4.** The collection of information means the collection of suspicious or unusual messages from all the employees of the Financial Service Provider, representatives (if any) and the contractual partners, and the systematization and analysis of the information provided therein.
- 7.5.** The main circumstances to consider when considering suspicious and unusual transactions are:
- 7.5.1. What is the suspicious fact in the operations or other circumstances;
- 7.5.2. Whether the employee of the Financial Service Provider is convinced that it is familiar with the customer to the extent necessary or whether additional information is required on it;
- 7.5.3. The employee in charge must make sure that it has complied with the prescribed procedure in the identification of the customer or its representative. It must be clarified if all the necessary information was provided, or if it was necessary to ask for information or otherwise specify it;
- 7.5.4. To find out if there are repeated manifestations of suspicious activity.
- 7.6.** If postponement of an act can significantly damage the parties, failure to do so is not possible or could prevent the seizure of the person committing money laundering or terrorist financing, the act will be carried out and, after that, the Contact Person shall notify the Financial Intelligence Unit. The Financial Intelligence Unit must be notified not later than within two business days of the identification or suspicion of any action or circumstances.
- 7.7.** For performing its duties the Contact Person has the right to access the information that is the basis or precondition of the business relationship, including the customer's identity and information, data or documents describing its business activities. The management board must also ensure that the Contact Person has the right to participate, if necessary, in the meetings of the board, if the Contact Person considers it necessary in the performance of its duties.
- 7.8.** The management board of the Financial Service Provider shall keep in written reproducible format all reports received from employees on suspicious and unusual transactions, as well as information and other related documents collected for the analysis of these messages, and notifications to the Financial Intelligence Unit, together with the time of transmission of the notice and the data of the employee who provided them.
- 7.9.** It is prohibited to inform the customer or the person involved in the transaction (incl. its representative and other related persons) who is being suspected about the notification of the Financial Intelligence Unit.
- 7.10.** The Contact Person shall forward the notice together with the necessary information to the Financial Intelligence Unit via the web form or X-Road service.<sup>5</sup> Information used to verify the person and the submitted data, as well as copies of the documents (if any) are added to the notice.

---

<sup>5</sup> Submission of notice electronically: <https://www.politsei.ee/et/organisatsioon/rahapesu/saada-teade.dot>

## **8. Procedure for inspecting compliance with the Guideline**

### **General requirements**

- 8.1.1. The management board is responsible for inspect compliance with the procedures contained in this Guideline.
- 8.1.2. The board is required to:
  - Analyze the results of work monitoring and checking compliance;
  - Assess the training needs of employees.
- 8.1.3. The management board must ensure regular training for that the employees whose duties include the establishment of business relations, regarding the obligations arising from this Act. The training must provide, in particular, information on modern methods of money laundering and terrorist financing and the risks involved.

### **Compilation of the inspection report**

- 8.1.4. The inspection report drawn up by the management board must include at least the following information:
  - Purpose of inspection;
  - Time of inspection;
  - Name and official title of the inspector;
  - Description of the inspection carried out;
  - Analysis of the results of the inspection or general conclusions of the performed inspection.
- 8.1.5. If the inspection reveals deficiencies in the Guideline or in its practical application, the inspection report shall include descriptions of the deficiencies together with an analysis of potential hazards associated with it. It also provides time to correct deficiencies, the measures that are desirable to remedy the deficiencies, and the timing of follow-up.
- 8.1.6. When performing the follow-up, an analysis of the results of the follow-up inspection and a list of the measures used to remedy the deficiencies will be included in the inspection report, indicating the time actually elapsed to remedy the deficiencies.

### **Training obligation**

- 8.1.7. In training provided to employee(s) an overview shall be provided of the modern methods of money laundering and terrorist financing and the associated risks.
- 8.1.8. The Contact Person introduces the Guideline to a new employee who is obliged to train in accordance with clause 6.1.3 at least within one week from the conclusion of the employment contract after the start of the new employee's employment. The employee confirms introduction with the Guideline by signature.
- 8.1.9. The management board's role is to ensure the annual training of employees. The exact time and place of training is determined by the board. The period between the two training sessions must not be more than 12 months. The board may ask the Contact Person to conduct training. The board may also invite a trainer who has sufficient knowledge to carry out the training. The Contact Person has the right to submit proposals to the management board regarding the trainers.
- 8.1.10. The board may, on a proposal from the Contact Person, also arrange training more often, in particular, for introducing and clarifying innovations arising from changes in the law.

\*\*\*