Finantsinspektsioon

Advisory Guidelines of Finantsinspektsioon
"Organisational solutions and preventive measures for credit and financial institutions to take against money laundering and terrorist financing"

The advisory guidelines have been established by resolution no. 1.1-7/172 of the Management Board of Finantsinspektsioon of 26 November 2018.

This document is translation from Estonian. In case of doubts about the used terminology please refer to the Guideline text provided in Estonian language. If application and interpretation problems arise upon application of the Guidelines, the principle of reasonableness must be followed in light of the purpose of these Guidelines and the principle of good faith must be upheld in accordance with the duty of due diligence expected of an obligated person.

TABLE OF CONTENTS

1. Competence of Finantsinspektsioon

1.1. Pursuant to § 3 of the Financial Supervision Authority Act (hereinafter the *FSAA*), Finantsinspektsioon conducts state financial supervision in order to enhance the stability, reliability, transparency and efficiency of the financial sector, to reduce systemic risks and to promote prevention of the abuse of the financial sector for criminal purposes, with a view to protecting the interests of customers and investors by safeguarding their financial resources, and thereby supporting the stability of the monetary system of the Republic of Estonia (hereinafter *Estonia*).

1.2. According to subsection 64 (2) of the Money Laundering and Terrorist Financing Prevention Act[1] (hereinafter the *MLTFPA*), Finantsinspektsioon exercises supervision over compliance with the MLTFPA and legislation adopted on the basis thereof by credit institutions and financial institutions that are subject to its supervision under the FSAA and in accordance with the legislation of the European Union. Finantsinspektsioon exercises supervision in accordance with the procedure provided for in the FSAA, taking account of the variations provided for in the MLTFPA.

1.3. Pursuant to subsection 57 (1) of the FSAA, Finantsinspektsioon has the right to issue advisory guidelines to explain legislation regulating the activities of the financial sector and to provide guidance to subjects of financial supervision.

2. Purpose, scope of application, underlying principles and definitions

2.1. Purpose

2.1.1. The purpose of these guidelines is to contribute to increasing the ability of obliged entities[2] to combat money laundering and terrorist financing with the ultimate goal of preventing the use of the financial system and economic space of Estonia for money laundering and terrorist financing and thereby increasing the trustworthiness and transparency of the business environment.

2.1.2. These advisory guidelines (hereinafter the *Guidelines*) explain the content of and compliance with the requirements provided for in the MLTFPA and legislative acts[3] directly related thereto with respect to obliged entities and understanding of risks associated with service provision as well as provide guidance to obliged entities in building up and functioning of the organisational solutions applied for the purpose of prevention of money laundering and terrorist financing.

2.1.3. The establishment of the Guidelines and implementation thereof by obliged entities reduces the probability of the Estonian financial sector being used for criminal purposes, decreases systemic risks and increases the stability, reliability and transparency of the financial sector.

2.2. Scope of application

2.2.1. The Guidelines are aimed at the credit and financial institutions providing services in Estonia that are obliged entities in respect of compliance with the requirements stipulated in the MLTFPA and that are subject to supervision by Finantsinspektsioon[4] (hereinafter the *obliged entity*). Such entities are:

[1] Money Laundering and Terrorist Financing Prevention Act. – RT I, 17.11.2017, 2 … RT I, 17.11.2017, 38.
[2] See point 2.2.1 of these Guidelines for the definition of the term 'obliged entity'.
[3] Within the meaning of these Guidelines, legislative acts directly related to the MLTFPA include directives and regulations of the European Union that have been transposed into the Estonian law by the MLTFPA as well as the recommendations of the Financial Action Task Force (hereinafter the *FATF*) and other guidelines that have served as a basis for the establishment of the relevant directives and regulations of the European Union (hereinafter the *legislative acts directly related to the MLTFPA*).
[4] Supervision subjects of Finantsinspektsioon are determined by the FSAA.

2.2.1.1. credit institutions[5];

2.2.1.2. payment institutions[6];

2.2.1.3. e-money institutions[7];

2.2.1.4. insurance undertakings[8];

2.2.1.5. insurance brokers[9];

2.2.1.6. fund management companies and investment funds established as public limited companies[10];

2.2.1.7. investment firms[11];

2.2.1.8. creditors and credit intermediaries[12];

2.2.1.9. Estonian branches (establishments) of foreign credit and financial institutions, which provide the service stipulated in points 2.2.1.1 to 2.2.1.8[13];

2.2.1.10. a central securities depository[14].

2.2.2. Finantsinspektsioon may establish annexes to these Guidelines in order to provide obliged entities with sector-based guidelines upon identification of the risks related to the provision of services by them. Finantsinspektsioon may amend or supplement the technical annexes to the Guidelines, except the sector-based guidelines specified in this point, without the inclusion of market participants or other experts.

2.2.3. These Guidelines are established along with the respective policy document of Finantsinspektsioon.

2.3. Underlying principles and definitions

2.3.1. The terms as used in these Guidelines have been defined in Division 2 of Chapter 1 of the MLTFPA,

[5] Within the meaning of point (1) of Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1–337).
[6] Within the meaning of the Payment Institutions and E-money Institutions Act (hereinafter the *PIEMIA*), excluding providers of payment initiation and account information services. Although the MLTFPA defines payment service providers as obliged entities, the only payment service providers subject to supervision by Finantsinspektsioon are authorised payment institutions.
[7] Within the meaning of the PIEMIA.
[8] Within the meaning of the Insurance Activities Act (hereinafter the *IAA*) and to the extent in which insurance undertakings provide services related to life insurance, excluding services related to insurance contracts for mandatory funded pension within the meaning of the Funded Pensions Act (hereinafter the *FPA*).
[9] Within the meaning of the IAA and to the extent in which insurance brokers are engaged in life insurance distribution or provide other services related to investing.
[10] Within the meaning of the Investment Funds Act and to the extent in which they are not engaged in the management of a mandatory pension fund within the meaning of the FPA.
[11] Within the meaning of the Securities Markets Act.
[12] Within the meaning of the Creditors and Credit Intermediaries Act.
[13] In English – establishment.
[14] A central securities depository is an obliged entity in situations where the latter arranges the opening of securities accounts and provides services related to register entries without the mediation of an account operator. Within the meaning of the MLTFPA and these Guidelines, a central securities depository is not a financial institution, but it is still subject to the relevant requirements and exceptions established for financial institutions when it serves customers. One of such exceptions is also the option provided for in subsection 27 (1) of the MLTFPA to open an account at the central securities depository, including a securities account, before the application of the due diligence measures where transactions cannot be made by the customer or in the name of the customer with the property held on the account until the full application of the due diligence measures specified in clauses 20 (1) 1)–3), considering that the due diligence measures must be applied as soon as reasonably possible.

Section 1 of Chapter I of Directive (EU) 2015/849 of the European Parliament and of the Council[15] (hereinafter *AMLD 4*), the glossary of FATF Recommendations 2012[16] and of FATF Methodology 2013[17] or guidelines and other guidance materials of European Supervisory Authorities[18]. If there is no management board, the provisions concerning the management board apply to 'senior management' or 'the director of a branch'.

2.3.2. Compliance with the money laundering and terrorist financing prevention requirements is, within the meaning of these Guidelines, all of the activities that the FATF expects from member states and obliged entities in the application of preventive measures, incl. prevention of corruption and prevention of the proliferation of weapons of mass destruction[19].

2.3.3. The requirements arising from effective legislation, international practice and the legislation directly related to the MLTFPA, the other advisory guidelines of Finantsinspektsioon and the guidelines and other guidance materials of the European Supervisory Authorities[20] must be taken into account upon the implementation of these Guidelines.

2.3.4. In the case of imperative requirements arising from legislation, the provisions of legislation must be adhered to. If the Guidelines are in conflict with legislation, the meaning and content of the MLTFPA and the legislation directly related thereto must be followed. In the case of legislation/source materials directly related to the MLTFPA that are in English, the original wording and meaning of these must be proceeded from.

2.3.5. The principle of proportionality and a risk-based approach must be proceeded from upon compliance with the Guidelines (the following is a non-exhaustive list and hereinafter referred to as the *risk appetite and risks arising from activities of the obliged entity).* This means that upon compliance with various requirements, the obliged entity takes into account the risks of money laundering and terrorist financing associated with their activities, business model and business strategy as well as the stipulated risk appetite. In general, the above is a consideration of the size of the obliged entity and the nature, scope and level of complexity of their activities and the services they provide, and:

2.3.5.1. the risks associated with the products and services offered, their volumes and complexity, incl. in different jurisdictions;

2.3.5.2. the risks of the customers consuming the products and services and the structure of the customer portfolio;

2.3.5.3. the risks of sales channels, incl. risks associated with outsourcing;

2.3.5.4. geographic risks, incl. presence in other countries or provision of services to cross-border

[15] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849. (19.11.2018)

[16] The FATF Recommendations (2012). Online: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html. (19.11.2018)

[17] The FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems (2013). Online: http://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html. (19.11.2018)

[18] In English – ESA, i.e. the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA).

[19] In English – Financing of proliferation. See FATF Recommendation 7 for additional explanations for financing of proliferation of weapons of mass destruction, considering that prevention of proliferation of weapons of mass destruction primarily refers to the manufacture, acquisition, development, export, reloading, mediation, carriage, storage or use of nuclear, chemical or biological weapons or other materials intended for the manufacture of said weapons.

[20] Incl. the general guidance materials concerning the organisation and activities of financial institutions.

customers from a distance.

An obliged entity places the above in the context of the risks highlighted by supervisory authorities, law enforcement agencies[21] and the state, which threaten Estonia, and European Union risks identified by the institutions[22] of the European Union[23], thereby considering the size of the obliged entity within the context of the entire market. The associated risks in another country as well as the entity's size in the financial sector of such other country must also be taken into account in the case of a group. The bigger the obliged entity, the higher the risks associated with their activities, etc., the more frequently the measures described in these Guidelines must be taken or the more extensive the measures taken must be.

2.3.6. In the case of problems of application and interpretation of the Guidelines the principle of reasonableness must be followed, interpreting the different points of the Guidelines in conjunction with each other and taking into account the purpose of these Guidelines. It is also necessary to act in good faith and in compliance with the due diligence expected from an obliged entity.

2.3.7. The 'comply or explain' principle applies to the Guidelines, pursuant to which the subject of supervision must be able to justify where necessary why they do not implement some points of the Guidelines or implement them partially.

2.3.8. It may be necessary to apply measures differing from the Guidelines or additional measures under specific circumstances in order to appropriately identify and manage money laundering and terrorist financing risks, which is why an obliged entity cannot justify compliance with legislation simply with the fact that the entity followed the principles established in these Guidelines word-for-word.

2.3.9. An obliged entity does not recuse itself in communication with customers from the issues related to the implementation of legislation that regulates the prevention of money laundering and terrorist financing or these Guidelines and explains, when necessary, the necessity of such requirements in public interests. If necessary, an obliged entity structures their customer service solutions in such a manner that the requirements arising from legislation and these Guidelines are integrated into the customer service solutions as well as possible, thereby guaranteeing the smoothest customer service solution possible whilst complying with the obligations arising from legislation and these Guidelines.

3. Organisational structure and risk management

3.1. General principles

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

3.1.2. The risk management solution of an obliged entity must correspond to the principle of proportionality, i.e. the size of the obliged entity and the nature, scope and level of complexity of their activity and services provided, incl. the risk appetite and risks arising from activities of the

[21] Incl. by the financial intelligence units.
[22] For example, the so-called supranational risk assessment (SNRA).
[23] Considering the fact that said risk assessments and documents are constantly changing, Finantsinspektsioon has not referred to specific documents in these Guidelines. However, Finantsinspektsioon points out that said assessments and documents may be included in guidelines, yearbooks and other documents.

obliged entity, allowing for the effective achievement of the objectives of regulative requirements and, above all, the prevention of the use of the Estonian financial system and economic space for money laundering and terrorist financing, thereby guaranteeing the reliability of the business environment.

3.1.3. Every manager and employee directly involved in the implementation of the MLTFPA and these Guidelines must have the professional skills, i.e. the knowledge, skills and experience that allows them to comply with the provisions of legislation and the Guidelines fully and with adequate accuracy according to the scope of their duties and they must have passed the training required therefor or be instructed in this by the obliged entity in any other manner.

3.2. Determination of risk appetite

3.2.1. The obliged entity prepares and regularly updates the risk appetite[24] document. The risk appetite document addresses the risk levels and types that are primarily associated with the higher-than-usual threat that a customer may perform transactions that deviate from their ordinary activities[25], incl. transactions and acts that are unusual and do not suggest reasonable economic activities. Such an estimate of deviation is based on the appropriate professional skills of the obliged entity.

3.2.2. The risk appetite document determines the set of risk levels and types that the obliged entity is ready to take in order to carry out their economic activities and achieve their strategic goals (in accordance with their business plan) and that the obliged entity is capable of taking considering their capital, risk management and control capacity and regulative restrictions.

3.2.3. The size of the obliged entity and the nature, scope and level of complexity of their activities and services provided, incl. the risks arising from activities of the obliged entity, are taken into account when the regularity of updating the risk appetite is decided. The risk appetite must also be reviewed if the obliged entity identifies changed or additional risks in their activities when a risk assessment is carried out, as well as if the organisational solution of the obliged entity is not or may not be capable of mitigating the associated risks appropriately any longer (one or several (key) employees have left, restructuring of the organisation, changes in the structure and volume of services, etc.).

3.2.4. The content and level of detail of the risk appetite document depend on the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risks arising from activities of the obliged entity as well as the desired level of risks and the potential threat of the associated risks to the activities of the obliged entity, considering thereby the risk and threat assessments of supervisory authorities, law enforcement agencies, the state of Estonia and the European Union.

3.2.5. The risk appetite document must primarily take into account the higher-than-usual risks and indicators given in the risk assessment of the obliged entity. This means the determination of the risk appetite for all appropriate business lines, business units and/or groups of products and services in the case of (i) different business lines or business units and/or (ii) products or services that are fully differentiated from each other[26].

---

[24] In specialist literature, risk appetite and risk tolerance are considered both synonyms and terms with different content. In the context of these Guidelines, risk tolerance is a part of risk appetite.

[25] A customer, product and service or another circumstance that in the opinion of the obliged entity require more frequent actions for the purpose of managing the risk of money laundering or terrorist financing and that are not limited merely to the collection of data upon the establishment of a business relationship and the updating of the data from time to time are, among others, deviating. A non-deviating situation may be, for example, a resident of Estonia that, in the course of their ordinary and everyday conduct, takes a loan, deposits money or uses the deposited money for everyday consumption.

[26] For the purposes of this point, products and services are, in general, the services provided by the persons specified in point 2.2.1 of these Guidelines. In the case of so-called banking services, the aspects associated with depositing (for a term and on demand) and separately with the provision of payment services must be taken into account separately when a current account is opened.

3.2.6. The risk appetite document must include at least the following:

3.2.6.1. the obliged entity determines the risks (measured) at the qualitative and quantitative levels, incl. the products, services, customers, sales channels and geographic risks that the obliged entity is prepared to take in their business activities or that they want to avoid. Among others, it is determined whether and to what extent the obliged entity intends to establish business relationships with entities from states outside the European Economic Area or with e-residents and which services and via which sales channels they are prepared to provide to them;

3.2.6.2. the obliged entity also determines the compensation mechanisms (measured) at the qualitative and quantitative levels for the mitigation of the risks taken. The maximum permitted set of risks is taken into account in the case of the compensation mechanisms, not the risks that the obliged entity actually takes at a specific moment, excl. in the cases stipulated in point 3.4.3.3 of these Guidelines. The compensation mechanisms are primarily the establishment of an appropriate organisational solution for the mitigation of the risks to be taken, but also, among others, the measures applied by way of capital or other liquid resources, etc.;

3.2.6.3. the risk management measures used to identify the cases where the qualitative or quantitative indicators specified in the risk appetite document have been exceeded or the activities that do not comply with the risk appetite document (adherence with risk appetite) as well as the situations where the compensation mechanisms do not correspond to the risk appetite (the obliged entity no longer tolerates the risks taken or to be taken in the future) and the measures for responding to such circumstances.

3.2.7. In the situations where the obliged entity is, as the parent company, a part of a larger group that provides financial services, the risk appetite document, incl. the risks (measured) at the qualitative and quantitative levels and the compensation mechanisms, must reflect the circumstances associated with the entire group[27]. And vice versa, if an obliged entity is a part of a group as a subsidiary, the risk appetite document must also take into account the relevant documents of the group, if any.

3.2.8. The document determining the risk appetite is established and approved in writing by the management board of the obliged entity by its resolution.

3.3. Risk assessment

3.3.1. An obliged entity prepares and regularly updates a risk assessment to identify, assess and analyse the risks of money laundering and, separately, of terrorist financing associated with their activities (differentiating between these two risks and assessing them separately is important). This means that an obliged entity must identify and clearly define which products and services or which ways can be used to take advantage of them for money laundering or terrorist financing (i.e. what the risk/threat is). This also covers strategic analyses to understand the organisation's bottlenecks (i.e. its vulnerability)[28].

3.3.2. The content and level of detail of the risk assessment depend on the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risks arising from activities of the obliged entity, as well as the size of the desired risks (risk appetite) and the potential impact of the associated threats on the activities of the obliged entity, considering thereby

[27] A group within the meaning of this point is restricted only to companies that provide financial services.

[28] For example, where do the customers come from and how; also where did the customers with whom business relationships have been extraordinarily (within the meaning of point 6.3 of these Guidelines) terminated come from and how; or with whom did the obliged entity refuse to establish a business relationship, because the customer did not submit data for due diligence or because money laundering or terrorist financing was suspected (within the meaning of point 6.1 of these Guidelines), etc.

the risk and threat assessments of supervisory authorities, law enforcement agencies, the state of Estonia and the European Union.

3.3.3. The size of the obliged entity and the nature, scope and level of complexity of their activities and services provided, incl. the risk appetite and the risks arising from activities of the obliged entity, are taken into account when the regularity of updating the risk assessment is decided. The risk assessment must also be reviewed if the obliged entity decides to change the services provided and products offered, use new or updated sales channels, offer their products or services to new markets or in new geographic locations or change their risk appetite in order to take more risks.

3.3.4. The risk assessment document must include at least the following:

3.3.4.1. at first, the obliged entity identifies the risks/threats arising from their activities as well as the risks/threats that may emerge in the near future, i.e. are foreseeable, and assesses and analyses their size and impact. The risks/threats are identified and assessed specifically as at the moment the risk assessment is carried out and separately considering the situation where the obliged entity had to take risks to the maximum extent permitted on the basis of the risk appetite. The obliged entity identifies, assesses and analyses at least the following risks:

i. customer risk;

ii. product, service or transaction risk, incl. new and/or future product, service or transaction[29] risk;

iii. risk related to the communication or mediation channels between the obliged entity and customers[30] or to delivery channels and sales of products, services or transactions, incl. such new and/or future channels[31];

iv. risk related to countries or geographic regions or jurisdictions;

3.3.4.2. thereafter, the obliged entity will determine the risk management model (compensation mechanisms) for the mitigation of the risks/threats arising from their activities and identify the residual risk as well as its size and the impact on the obliged entity after the implementation of the compensation mechanisms. The size of the maximum risk/threat arising from activities, i.e. the situation where the obliged entity should take risks to the maximum extent permitted on the basis of the risk appetite, excl. the case stipulated in point 3.4.3.3 of these Guidelines, is taken into account in the case of compensation mechanisms. The compensation mechanisms are primarily the establishment of an appropriate organisational solution for the mitigation of the risks to be taken, but also, among others, the measures applied by way of capital or other liquid resources, etc.;

3.3.5. On the basis of the risk assessment, the obliged entity also determines the situations and conditions whereby the obliged entity may apply enhanced or simplified due diligence measures in economic activities and defines the content and essence of enhanced or simplified due diligence measures.

3.3.6. In the situations where the obliged entity is, as the parent company, a part of a larger group that provides financial services, the risk assessment document, incl. risks/threats affecting the activities of the obliged entity and the compensation mechanisms, must reflect the circumstances associated

[29] The money laundering and terrorist financing risk of new and/or future products, services or transactions can also be assessed as a part of product governance.
[30] IT channels and channels that require physical contact must all be taken into account.
[31] The money laundering and terrorist financing risk of new and/or future communication or mediation channels or delivery channels of products, services or transactions must be assessed as a part of product governance.

with the entire group[32] (incl. the branch(es), if any). And vice versa, if an obliged entity is a part of a group as a so-called subsidiary, the risk assessment document must also take into account the relevant documents of the group, if any.

3.3.7. If the obliged entity has no group companies in other countries, but the obliged entity has, in the risk appetite document or in any other manner, set itself the goal to serve customers originating from[33] other countries or regions (incl. in the case of provision of a cross-border service and concentration on serving certain customer groups[34]), the risk assessment document must also reflect the risks specified in point 3.3.4.1 associated with these countries or territories.

3.3.8. The measures of risk management with which significant changes in the risks arising from activities of the obliged entity are identified within reasonable time are determined in the risk assessment document.

3.3.9. The risk assessment document is established and approved in writing by the management board of the obliged entity by its resolution.

3.4. Activities of the management board[35]

3.4.1. The managers of an obliged entity must act with the foresight and competence expected from them and according to the requirements set for their positions, proceeding from the interests of the obliged entity and their customers, and ensure that the Estonian financial system and economic space are not used for money laundering and terrorist financing.

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

3.4.2.1. takes into account the provisions of point 3.2 of these Guidelines and guarantees the preparation of risk appetite and risk assessment documents and their regular reviews;

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

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

[32] A group within the meaning of this point is restricted only to companies that provide financial services.
[33] The term 'originating from' is, within the meaning of this point, a situation where a person has the citizenship of said country or territory or their place of residence or registered office is in said country or territory.
[34] For example, aiming services and products at customers originating from the former states of the Soviet Union. Also, within the meaning of this footnote, 'originating from' means the connection selected by the obliged entity itself, incl. the customer's place of birth, place of residence or business, habitual residence, place related to the member(s) of the management board or beneficial owner(s), etc.
[35] In a situation where the obliged entity has no management board, the term 'management board' is to be read as 'senior management' or 'director of the branch' in the context of these Guidelines.

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

3.4.3.2. establishes rules of procedure for compliance with the MLTFPA and the legislative acts directly related thereto and the principles specified in these Guidelines (hereinafter also *internal procedures*) and guarantees that the employees directly involved in compliance with the requirements of the MLTFPA and these Guidelines act in conditions where they are fully aware of the requirements of the MLTFPA and these Guidelines;

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

3.4.3.4. in addition to the creation of an organisational solution and the allocation of adequate human resources, ensures that the functional separation of different lines of defence and management of conflicts of interest are guaranteed. This obligation calls for, among others, regular[36] assessment of whether the bases for remuneration of managers and employees, incl. economic interests in respect of third parties[37], will motivate them to waive or make concessions in compliance with the provisions of legislation and the Guidelines.[38] The management board guarantees solution for identification, assessment, management and reduction of compliance or non-compliance with the aforementioned principles;

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

3.4.4. The management board of the obliged entity must organise the effective functioning of the internal control system and ensure control that the activities of the obliged entity, their managers and employees comply with legislation and the documents approved by the managing bodies as well as

[36] Regular means at least once a year.

[37] These third parties may be, among others, family members and the persons who consume the services of the obliged entity and relationships with third parties that have emerged on personal and business grounds.

[38] In respect of this obligation, see also the guidelines on internal governance of the European Banking Authority, and particularly paragraphs 103–116, which in the context of these Guidelines are relevant to all obliged entities. Online: https://www.fi.ee/public/pp_nr_08_Guidelines_on_Internal_Governance_EBA-GL-2017-11_ET.pdf. (19.11.2018)

good practices. The management board of the obliged entity thereby regularly assesses the efficiency of the internal procedures implemented for compliance with the MLTFPA and these Guidelines and ensures internal control of such compliance.

3.4.5. The obliged entity appoints the person(s) who is (are) responsible for performance of the obligations stipulated in the MLTFPA at the level of the management board[39]. Whereby:

3.4.5.1. the competency and responsibility of said person must arise from the internal documents (such as the rules and regulations of the management board, job descriptions of members of the management board, service agreements, etc.) that regulate the duties of members of the management board in a manner that is transparent and unambiguous;

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

3.4.6. The management board of the obliged entity takes minutes of the decision-making process with which they perform the measures implemented upon the assumption of the obligations specified in this sub-chapter (point 3.4 of these Guidelines), the measures taken for implementation and other measures taken for the prevention of money laundering and terrorist financing.

3.5. Building the organisation by the three lines of defence principle

3.5.1. General principles

3.5.1.1. The organisational structure of the obliged entity for the purposes of the risk management matrix must correspond to their size and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and the associated risks, and must be built by the three lines of defence principle. The organisational structure of the obliged entity corresponds to the full understanding of risks and their management. Risk management is comprehensive and covers all of the activities of the obliged entity.

3.5.1.2. In the development of the risk management matrix, the obliged entity considers the principles of separation of functions and prevention of conflicts of interests. In order to identify and manage conflicts of interests, the obliged entity:

i. establishes a procedure for management and prevention of conflicts of interest, which stipulates legal, technical and organisational measures, considering the nature, scope and level of complexity of the activities of and services provided by the obliged entity, incl. the risk appetite and risks arising from activities of the obliged entity. This covers the principles of remuneration of employees (incl. persons in authorisation or other legal relationships) and managers;

ii. avoids situations in the case of which the personal (incl. economic) interests of owners, managers and employees (incl. persons in authorisation or other legal relationships) and customers are in conflict with the interests of the obliged entity, which primarily covers

[39] The 'senior management' or director of the branch is meant in the context of these Guidelines in the case of branches.

the interest to comply with the requirements of money laundering and terrorist financing prevention arising from legislation and other guidelines, incl. these Guidelines;

iii. asks their employees[40] (incl. persons in authorisation or other legal relationships[41]) and managers[42] to provide data about their economic interests from the viewpoint of money laundering and terrorist financing prevention and assesses the data presented therein from the viewpoint of a conflict of interests. The obliged entity regularly updates these declarations of economic interests;

iv. identifies and analyses whether the persons who lead customers to the obliged entity (i.e. agents, distributors, etc.) have interests in respect of the customers (e.g. provide them with legal services, accounting services, service related to the establishment of companies and other legal structures, etc.), which is why the person who leads the customer to the obliged entity has a conflict of interests between the obliged entity and the customer. In the case of such a conflict of interests, the management of which must be presumed from the obliged entity, the obliged entity takes measures to manage such a conflict of interests, which in some cases lies in avoiding it. In any case, the obliged entity is ready to justify the measures taken to Finantsinspektsioon and explain the content and scale of the conflict of interests. In the case of outsourcing of activities or reliance, point 4.8.1 or 4.8.2 of these Guidelines will also apply, respectively.

3.5.1.3. The volume and extent of compensation mechanisms, i.e. the need to and scope of use of IT solutions and the number of jobs filled in various lines of defence, must also comply with the size of the obliged entity and the nature, scope and level of complexity of their activities and services provided, incl. the risk appetite and associated risks.

3.5.1.4. The organisational structure of the obliged entity must be justified and efficient, and not unreasonably or unsuitably complicated and non-transparent. The obliged entity understands the goals and activities of different units as well as the links and relationships between them.

3.5.1.5. Reporting and subordination lines must be guaranteed in such a manner that all employees know their place in the organisational structure and their duties.

3.5.1.6. The employees of an obliged entity must act with the foresight and competence expected from them and according to the requirements set for their positions, proceeding from the interests and goals of the obliged entity, and ensure that the Estonian financial system and economic space are not used for money laundering and terrorist financing. Obliged entities must establish measures for assessing the suitability of employees before they are hired.

3.5.1.7. If the risk management function is outsourced, the principles specified in point 4.8.1 of these Guidelines apply with the relevant variations and the provisions established in the advisory guideline of Finantsinspektsioon "Requirements for outsourcing by subjects of financial supervision" and § 24 of the MLTFPA must be followed.

3.5.2. First line of defence

3.5.2.1. The first line of defence is a part of the risk management system that is related to the structural units with whose activities risks are associated and that must identify and assess these risks,

[40] Such employees are, among others, persons who come in contact with customers whose risk is higher than usual and who have the right to make decisions in respect of customer relationships involving a risk that is higher than the usual risk or in circumstances related to this. Also any other persons who deal with the management of the risks arising from customer relationships in terms of money laundering prevention irrespective of the customer's risk level.
[41] Irrespective of the customer's risk level.
[42] *Ibid*.

their specific features and scope and that manage these risks by way of their ordinary activities, primarily by way of application of due diligence measures. The risks arising from the activities of and provision of services by the obliged entity belong to the first line of defence. They are the managers (owners) of these risks and responsible for them. This means that the application of due diligence measures upon the establishment of customer relationships (within the meaning of point 4.3 of these Guidelines) and the ordinary monitoring of customer relationships (within the meaning of point 4.4 of these Guidelines) is a function of the first line of defence.

3.5.2.2. The first line of defence must have good knowledge of the customer and the specific features of their activities and business activities. This way, the employees in the first line of defence must be aware of or make themselves aware of the specific features of the different business activities of customers and the risks associated with them[43] if the obliged entity has decided to provide services to such customers. The goal is to identify transactions in the customer's activities that are suspicious or unusual or do not correspond to reasonable economic objectives, or transactions that refer to such circumstances, so they can be referred to the second line of defence for analysis.

3.5.2.3. The management board of the obliged entity assesses, when structuring the organisational solution, which cases and situations require the inclusion of IT systems or human resources in the work of the first line of defence for the appropriate management of risks (e.g. the inclusion of personal wealth managers when serving high-risk customers and/or customers who perform transactions of high value in order to give customers an appropriate, constant and enhanced attention). In any case, the principle highlighted in points 3.5.2.1, 3.5.2.2 and other points of these Guidelines must be complied with, i.e. the obliged entity has adequate knowledge of the customer and their activities to be able to identify suspicious and unusual transactions.

3.5.2.4. The duty of the first line of defence is, in the case of suspicion, to refer the identified risks, incl. so-called red flags in the form of suspicious and unusual transactions, to the second line of defence of risk management and, if necessary, directly to the management board of the obliged entity. In this manner and proceeding from the principle of separation of functions, the first line of defence does not deal with the extraordinary management of risks, i.e. primarily with the analysis of suspicious and unusual transactions. The first line of defence refers all suspicious or unusual circumstances and transactions, incl. those that do not refer to reasonable economic activities, to the second line of defence for risk management and further decisions.

3.5.3. Second line of defence, incl. the function of compliance officer

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

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

3.5.3.3. The task of compliance is to help the first line of defence as the owners of risk to define the places where risks manifest themselves (e.g. analysis of suspicious and unusual transactions, for which compliance employees have the required professional skills, personal qualities, etc.) and

[43] Customers, services and products, sales channels and geographic risks.

to help the first line of defence manage these risks efficiently. The second line of defence does not engage in taking risks.

3.5.3.4. Risk policy is implemented and the risk management framework is controlled via the risk management function. The performer of the risk management function ensures that all risks are identified, assessed, measured, monitored and managed, and informs the appropriate units of the obliged entity about them. The performer of the risk management function for the purposes of money laundering and terrorist financing prevention primarily performs the duties specified in points 3.2.6.3 (adherence to risk appetite and control of risk tolerance), 3.3.8 (identification of changes in risks), 3.4.3.1 (overview of associated risks), etc. of these Guidelines.

3.5.3.5. The compliance officer usually operates as a part of compliance or as a part of the second line of defence. Whereby:

i. the functions of the compliance officer may be performed by one or several employees and/or a structural unit with the relevant functions. If the functions of a compliance officer are performed by a structural unit, the head of the relevant structural unit is responsible for the performance of said functions;

ii. only a person who has the education, professional suitability, abilities, personal qualities and experience required for performance of the duties of a compliance officer and impeccable professional and business reputation may be appointed as a compliance officer by the management board of the obliged entity. The required abilities, skills and experience are assessed on the basis of the person's function and role in the structure, e.g. employees who identify suspicious and unusual transactions as part of the second line of defence must have acquired an education in economics, law or business or passed the relevant in-service training, etc., which helps with the development of the skills directly required to understand complicated, high-value and unusual transactions that do not have a reasonable economic purpose. The compliance officer must receive constant training for this;

iii. the placement of the compliance officer in the organisational structure of the obliged entity must be appropriate for compliance with the requirements of money laundering and terrorist financing prevention arising from legislation. However, upon the establishment of the institution of compliance officer, it is necessary to ensure that they report directly to the management board of the obliged entity and are as independent as possible from business processes[44];

iv. the compliance officer must have the required competency, tools and access to the relevant information in all structural units of the obliged entity. Primarily, this means access to the information that is the basis or precondition for the establishment of business relationships, incl. the information, data or documents that reflect the customer and their economic activities. The management board also ensures the compliance officer the right to attend the meetings of the management board if the compliance officer considers it necessary for the performance of their functions;

v. the compliance officer:

– organises the collection and analysis of transactions or circumstances that are unusual or related to suspicions of money laundering or information that refers

[44] The independence of the compliance officer from business processes does not mean that the latter may not advise or train their co-workers for the purpose of ensuring the compliance of the activity of managers and employees with the requirements of the MLTFPA and these Guidelines.

terrorist financing, which have become evident in the activities of the obliged entity. For this purpose, retains all reports received from employees on suspicious and unusual transactions as well as the information collected for analysing these reports and other related documents, in a format that can be reproduced in writing;

- reports to the Financial Intelligence Unit in the event of suspicion of money laundering or terrorist financing. This includes the obligation to retain the reports sent to the Financial Intelligence Unit in a format that can be reproduced in writing[45] with the time when the report was sent and the details of the employee who sent the report;

- prepares written overviews on compliance with money laundering and terrorist financing prevention requirements to the management board. An overview may be separate, i.e. only cover the roles of the compliance officer's function or a part of the general second line of defence statement with the compliance (and risk management) function, complying separately or with other functions with the requirements and regularity specified in point 3.5.3.7 of these Guidelines;

- performs other duties that are directly related to the prevention of money laundering and terrorist financing and that have not been assigned to compliance or risk management;

vi. the appointment of the compliance office is approved by the Financial Intelligence Unit;

vii. the contact details of the compliance officer are sent to Finantsinspektsioon and the Financial Intelligence Unit. The obliged entity informs Finantsinspektsioon within reasonable time about the appointment of a new compliance officer or any changes in their contact details.

3.5.3.6. The compliance and risk control employees involved in the prevention of money laundering and terrorist financing (if they are not parts of the function of the compliance officer) must also comply with the same requirements set for the compliance officer that are stipulated in sub-point 2 of point 3.5.3.5 of these Guidelines.

3.5.3.7. The second line of defence must prepare regular written overviews for the management board of the obliged entity. The overviews may be divided between the persons performing the compliance function, the compliance officer's function and the risk control function, but they may also be presented as a single overview. The regularity of the overviews depends on the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and risks arising from activities of the obliged entity, but takes place at least once a quarter, incl. extraordinarily if necessary. The overviews together or separately must highlight at least the following:

i. modern methods of money laundering and terrorist financing and specific typologies/cases and trends, the risks associated therewith, incl. impact on the obliged entity (both the impact of risks and the need to manage these risks via the organisational solution);

ii. the risks highlighted by supervisory authorities, law enforcement agencies and the state of Estonia, which threaten Estonia, and the risks identified by the institutions of the European Union, which threaten the European Union, incl. their impact on the obliged

[45] I.e. allows for it to be reproduced later.

entity (both the impact of risks and the need to mitigate these risks via the organisational solution);

iii. the risks arising from the activities of and provision of services by the obliged entity and the volumes of the services provided as well as possible changes in the risks and volumes;

iv. adherence to risk appetite;

v. incidents related to the prevention of money laundering and terrorist financing;

vi. statistics related to circumstances and transactions that are suspicious and unusual and related to suspicions of money laundering and terrorist financing (incl. internal reports and reports sent to the Financial Intelligence Unit) and analysis done on the basis of the statistics, and placing this in the context of the risks arising from the activities of and services provided by the obliged entity;

vii. estimates of the adequacy of the compensation mechanisms of the obliged entity (incl. IT systems and human resources);

viii. proposals for amendment or supplement of the measures taken by the obliged entity for the prevention of money laundering and terrorist financing, risk appetite and/or risk assessments;

ix. proposals for terminating or suspending the offer of certain products or the provision of certain services for as long as the compensation mechanisms of the obliged entity or other capabilities have been made to correspond to the risks taken;

x. any other circumstances required to identify compliance with the requirements for prevention of money laundering or terrorist financing.

In the event of occurrence of certain risks or incidents, they must be reported and overviews must also be made extraordinarily and in the *ad hoc* version, whilst the second line of defence decides in each case whether the preparation of an extraordinary overview is necessary and the related circumstances.

3.5.3.8. The obliged entity presents the report(s) and/or overviews for the management board of the person who performs the function of compliance or risk management to Finantsinspektsioon if they identify significant omissions in the measures and actions taken for the prevention of money laundering and terrorist financing.

3.5.4. Third line of defence

3.5.4.1. The independent and effective internal audit function comprises the third line of defence of the obliged entity[46]. The internal audit function may be performed by one or several employees and/or a structural unit with the relevant functions[47]. In the case of a structural unit, the entire unit must comply with the requirements set out below and the head of the structural unit is responsible for the performance of the functions.

[46] The management board of the obliged entity is also a part of the third line of defence in certain cases. However, the internal audit function is meant in point 3.5.4 of these Guidelines.
[47] The internal audit function may be outsourced to a third party.

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

3.5.4.3. The person who performs the internal audit function or their head if it is a structural unit must have the relevant professional standard (attestation) for the performance of their duties and, among others, the required education, suitability, necessary capabilities, personal qualities, knowledge and experience, and impeccable professional and business reputation. The person who performs the internal audit function must always be informed about the risks and trends of money laundering and terrorist financing both at the general level and in the context of the obliged entity.

3.5.4.4. The internal audit function assesses, among others, whether:

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

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

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

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

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

vi. the methods of the obliged entity (as 'cross-obliged entity' methods and as a holistic[48] view) are appropriate and adequate for the prevention of money laundering and terrorist financing, and they correspond to the organisation's needs and the expectations of supervisory authorities.

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

3.5.4.6. If the internal audit function is outsourced, the obliged entity ensures compliance with, among others, the requirements arising from these Guidelines, primarily from point 3.5.4.4 of thereof. If the internal audit function is outsourced, the obliged entity (usually the supervisory board of the obliged entity in cooperation with the management board) constantly assesses whether outsourcing the internal audit function is justified and the efficiency of the internal audit.

[48] In English – holistic view.

3.5.4.7. The obliged entity presents the internal audit report(s) to Finantsinspektsioon if they identify significant omissions in the measures and actions taken for the prevention of money laundering and terrorist financing.

3.6. Business continuity and events of operational and reputational risk

3.6.1. The obliged entity develops the business continuity measures and rules of procedure of the compensation mechanisms of the (IT) systems created for the prevention of money laundering and terrorist financing.

3.6.2. The measures taken must at least cover the activities required to ensure the business continuity of compensation mechanisms as well as the activities required in the situations where the business continuity of compensation mechanisms is discontinued.

3.6.3. The obliged entity notifies Finantsinspektsioon about the business continuity incidents of compensation mechanisms and the measures taken as soon as possible.

3.6.4. The obliged entity also informs Finantsinspektsioon about other significant events of operational and reputational risk related to the prevention of money laundering and terrorist financing as soon as possible.

3.7. Training

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

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

3.7.2.1. the principles specified in the risk appetite document of the obliged entity[49];

3.7.2.2. the risks arising from the activities of and services provided by the obliged entity[50], incl. risks foreseen in the future;

3.7.2.3. the obligations stipulated in the rules of procedure;

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

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

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

3.7.4. The regularity of training depends on the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and risks arising from

[49] Considering the document prepared on the basis of point 3.2 of these Guidelines.
[50] Considering the document prepared on the basis of point 3.3 of these Guidelines.

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

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

3.8. Establishment of and requirements for rules of procedure

3.8.1. The obliged entity establishes rules of procedure for the efficient mitigation and management of risks related to money laundering and terrorist financing. The obliged entity implements the established rules of procedure. The complexity and structure of rules of procedure must correspond to the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and risks arising from activities of the obliged entity.

3.8.2. The rules of procedure include at least the following:

3.8.2.1. the procedure for assessing the risks arising from the activities of the obliged entity, as well as the procedure for identification and management of the risks associated with new and existing technologies and services and products, incl. new or non-traditional sales channels and new or emerging technologies;

3.8.2.2. the procedure for prevention of conflicts of interests (see also point 3.5.1.2 of these Guidelines);

3.8.2.3. the model for the identification and management of the risks arising from the customer and their activities and the determination of the risk profile of the customer (see also point 4.2 of these Guidelines);

3.8.2.4. the procedure for the management of the risks of money laundering and terrorist financing, i.e. a procedure for the performance of all of the obligations stipulated in point 4 of these Guidelines, i.e. among others the procedure for application of due diligence measures to customers and the procedure for application of simplified due diligence measures and enhanced due diligence measures. The activities of the different lines of defence of risk management[51] which the obliged entity carries out in order to comply with various due diligence measures upon the establishment of a customer relationship and upon the occasional conclusion and mediation of transactions must be described in the rules of procedure. The procedure specified in this point includes, among others, a guideline on how to efficiently ascertain whether a person is a politically exposed person or local politically exposed person or a person subject to international sanctions or a person who is originally from or whose place of residence or location is in a high-risk third country or in a country that meets the conditions stipulated in subsection 37 (4) of the MLTFPA;

3.8.2.5. the duties, rights and roles of the person who performs the functions of compliance, incl. the compliance officer, and risk management, which are not covered under point 3.8.2.4 of these Guidelines. The provisions of clause 3.5.3 of these Guidelines must be taken into account in the case of duties;

3.8.2.6. the procedure for the collection and retention of data and for making them accessible;

[51] For example, if the identification of a natural person is described in the rules of procedure, it has to be described which data are collected and who collects and checks them.

3.8.2.7. the situations where the employees of the first line of defence of risk management must notify the compliance officer about suspicious or unusual transactions;

3.8.2.8. the procedure for refusal to establish a business relationship or refusal of an occasional transaction (within the meaning of point 6.1 of these Guidelines), the procedure for exercising the right to refuse to conclude a transaction (within the meaning of point 6.2 of these Guidelines) and the procedure for extraordinary termination of a business relationship (within the meaning of point 6.3 of these Guidelines), incl. (i) who makes the relevant decisions, (ii) who implements the relevant decisions (who and when closes the relevant accesses of the customer, makes the relevant notices in the system, informs the customer, etc.), (iii) how the compliance officer is informed about the circumstances and (iv) reporting to the Financial Intelligence Unit when appropriate;

3.8.2.9. the procedure for reporting to the Financial Intelligence Unit (within the meaning of point 7 of these Guidelines), incl. (i) reporting on internally suspicious and unusual transactions or circumstances, (ii) the methodology and the guideline from which the compliance officer proceeds when analysing suspicious and unusual transactions or circumstances, and (iii) the methodology and the guideline in the case the obliged entity suspects money laundering or terrorist financing, or an unusual transaction or circumstance is detected;

3.8.2.10. the procedure for outsourcing (see point 4.8.1 of these Guidelines) and relying on another person (see point 4.8.2 of these Guidelines);

3.8.2.11. the procedure for training the employees of the obliged entity who are involved in the prevention of money laundering and terrorist financing as well as the senior management, incl. the management board, and the persons to whom activities have been outsourced;

3.8.2.12. the procedure for the establishment and continuation of correspondent relationships if relevant (see point 4.9 of these Guidelines);

3.8.2.13. the procedure for renewal of rules of procedure;

3.8.2.14. the procedure for performance of the other obligations arising from these Guidelines.

3.8.3. In order to check compliance with the rules of procedure, the obliged entity establishes internal control rules that describe the procedure for the functioning of the internal control system, incl. the procedure for implementation of an internal audit and, where necessary, compliance, where the procedure for checking employees is described, among others.

3.8.4. The obliged entity organises compliance with and implementation of the rules of procedure and the internal control rules by the employees of the obliged entity.

3.8.5. The obliged entity regularly checks that the established rules of procedure and internal control rules are up to date, incl. in confluence with the established risk appetite and risks arising from activities, and establishes new rules of procedure or internal control rules or updates them, if necessary.

3.8.6. The obliged entity appoints the person(s) and structural units that must follow the rules of procedure and separately the person(s) or structural unit responsible for updating, amending or preparing them.

3.8.7. The rules of procedure and internal control rules may be contained in a single document or in multiple documents, but they must be approved in writing by the management board (or supervisory board if this arises from the nature of the document) of the obliged entity. The rules of procedure are made permanently accessible to employees and they are introduced to employees.

3.9. Risk management and measures in a group

3.9.1. In the event of groups where the obliged entity is in the function of a parent company[52], the obliged entity's duty and responsibility is to ensure that the principles of these Guidelines, especially the ones concerning the organisational structure and the group-wide rules of procedure, are applicable to the entire group[53].

3.9.2. If the obliged entity belongs to a group as a parent company and as a subsidiary, the risk appetite document and risk assessment document of the obliged entity must consider the respective documents and assessments of the other members of the group (see also points 3.2.7 and 3.3.6 of these Guidelines).

3.9.3. In the case of a group, the group-wide rules of procedure must cover at least the following:

3.9.3.1. the group-wide procedure for assessment of risks and determination of risk appetite;

3.9.3.2. a description of compensation mechanisms that would comply with the risks of the group as well as each group company and with the group-wide risk appetite and the risk appetite of each company;

3.9.3.3. a description of the organisational solution for the prevention of money laundering in the group, which among others includes the principle of the three lines of defence (see also point 3.5 of these Guidelines). In the case of a group, the subordination of the different lines of defence (especially the second and third lines of defence) and the reporting lines with the unit of the same line of defence that performs the group-wide function must also be established;

3.9.3.4. the measures and procedure for exchanging internal information about money laundering and terrorist financing prevention in the group. This also covers the exchange of information related to due diligence measures and management of the risk of money laundering and terrorist financing, which includes the analysis of suspicious and unusual transactions and circumstances as well as the report submitted to the Financial Intelligence Unit and the documents serving as a basis therefor. This also covers the measures of keeping up to date with the applicable risks (in relation to all companies belonging to the group). Exchanging the above information should only be limited to situations where it is appropriate and necessary for risk management;

3.9.3.5. the procedure for personal data protection and the procedure for ensuring the confidentiality and secrecy of transmitted data (to avoid, among others, situations of tipping-off[54]) and the restrictions on the use of information transmitted in the group;

3.9.3.6. description of the measures on the basis of which the suitability of employees is assessed before the commencement of their employment (see also point 3.5.1.6 of these Guidelines);

3.9.3.7. description of the procedure for training the employees who are involved in the prevention of money laundering and terrorist financing as well as the senior management, incl. the management board, and the persons to whom activities have been outsourced;

---

[52] In English – parent company.

[53] Entities belonging to a group mean representations, agents (especially payment institutions and e-money institutions), branches and subsidiaries with majority holdings that are obliged entities within the meaning of the MLTFPA and that are based in Estonia and outside Estonia. The MLTFPA defines a group as a group of undertakings which consists of a parent company, its subsidiaries within the meaning of § 6 of the Commercial Code, and the entities in which the parent company or its subsidiaries hold a participation, as well as undertakings that constitute a consolidation group for the purposes of subsection 27 (3) of the Accounting Act.

[54] In English – tipping-off.

3.9.3.8. the internal control rules that cover the procedure and measures for the functioning of the independent audit function. This also covers the measures taken to ensure that the group companies implement group-wide policies and take into account the established risk appetite in other respects.

3.9.4. The group-wide rules of procedure and the internal control rules for supervision of compliance therewith are applied irrespective of whether the group companies are all located in the same country or in different countries. The obliged entity ensures that group-wide rules of procedure and the internal control rules for supervision of compliance therewith take the law of another Member State of the European Union into account to appropriate extent.

3.9.5. The obliged entity and the companies belonging to their group do not apply the exceptions to due diligence measures established and permitted or simplified due diligence measures permitted in another country if this does not comply with the obliged entity's risk assessment or the national threat assessment of Estonia or the national threat assessment published in the country of operation of a member of their group, incl. the risk assessments of the law enforcement agencies or supervisory authorities of the European Union, Estonia or such other country.

3.9.6. A company belonging to the obliged entity's group and operating in another European Union state must respect and comply with the law applicable in such Member State.

3.9.7. The obliged entity must ensure that the due diligence measures applied in their groups located in third countries and the requirements for collection and retention of data comply with the requirements set out in the MLTFPA and these Guidelines. Finantsinspektsioon must be immediately informed in a situation where compliance with such requirements is not possible due to the features of local laws and additional measures must be taken for the prevention of the risks of money laundering and terrorist financing. The aforementioned additional measures must efficiently manage the associated money laundering and terrorist financing risks.

3.9.8. The obliged entity that has a branch or representation or subsidiary in a high-risk third country implements the measures stipulated in point 4.10 of these Guidelines and carries out extraordinary (internal and external) audits, and also weighs and assesses the need to close the branch, representation or subsidiary in said country unless the associated risks can be efficiently mitigated. An obliged entity that decides not to close such a branch, representation or subsidiary must inform Finantsinspektsioon about this and submit the explanations and reasons for the decision made.

4. Due diligence measures in respect of customers or third parties

4.1. General principles

4.1.1. One of the main obligations of the obliged entity in the prevention of money laundering and terrorist financing is the application of preventive measures, i.e. due diligence measures. The primary purpose of application of due diligence measures is to prevent the placement, layering and integration, etc. of criminal proceeds in the various stages of money laundering[55], prevent the financing of terrorism from illegal or legal sources of money, etc. Thus, the main goal is to ensure the trustworthiness and transparency of the Estonian business environment and prevent the use of the Estonian financial system and economic space for money laundering and terrorist financing.

4.1.2. The obliged entity has applied due diligence measures adequately if the obliged entity has the inner conviction that they have complied with the obligation to apply due diligence measures. The principle of reasonability is observed in the consideration of inner conviction. This means that the obliged entity must, upon the application of due diligence measures, acquire the knowledge,

[55] In English – placement, layering and integration.

understanding and conviction that they have collected enough information about the customer, the customer's activities, the purpose of the business relationship and of the transactions carried out within the scope of the business relationship, the origin of the funds, etc., so that they understand the customer and customer's (business) activities, thereby taking into account the customer's risk level[56], the risk associated with the business relationship and the nature of such relationship (i.e. the risk profile of the business relationship). Such level of conviction must make it possible to identify complicated, high-value and unusual transactions and transaction patterns that have no reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question (see point 4.4.2 of these Guidelines and Annexes 1 and 2 to these Guidelines).

4.1.3. The application of due diligence measures divides into due diligence upon the establishment of a business relationship and the ongoing monitoring of a business relationship. The list of due diligence measures stipulates the minimum criteria and its content is imperative. The obliged entity may also implement other due diligence measures not stipulated by law proceeding from the customer's area or region of activity, the specific features of the transaction and the associated risks.

4.1.4. Upon the establishment of a business relationship

4.1.4.1. the due diligence measures taken are:

i. identification of a customer or a person participating in an occasional transaction and verification of the submitted information based on information obtained from a reliable and independent source, incl. using means of electronic identification and of trust services for electronic transactions (see points 4.3.1 and 4.3.2 of these Guidelines).

ii. identification and verification of a customer or a person participating in an occasional transaction and their right of representation (see point 4.3.1 of these Guidelines).

iii. identification of the beneficial owner and, for the purpose of verifying their identity, taking measures to the extent that allows the obliged entity to make certain that they know who the beneficial owner is, and understands the ownership and control structure of the customer or of the person participating in an occasional transaction (see point 4.3.3 of these Guidelines);

iv. gathering information on whether a person is a politically exposed person, their family member or a person known to be close associate (see point 4.3.4 of these Guidelines);

v. identification of the source and/or origin of wealth if appropriate (see point 4.3.5 of these Guidelines);

vi. understanding of business relationships or an occasional transaction and, where relevant, gathering additional information thereon (see point 4.3.6 of these Guidelines).

4.1.4.2. The purpose of application of due diligence measures is to comply with the Know-Your-

[56] For example, in a situation where the customer's risk level is high, a vague explanation of the source and origin of funds (the funds are the customer's savings, own funds, raised loan, earned money, etc.) cannot be considered sufficient. In the case of a high risk level, the obliged entity must apply enhanced due diligence measures, incl. take additional measures to make sure the data are correct. In this manner, the submitted data must give the obliged entity the inner conviction (i.e. proceeding from the principle of reasonability, it is possible to assume that a third party would have also been convinced under the same circumstances, i.e. on the basis of the same information) that they know why and, when necessary, for which purpose and within the scope of which economic or legal relationships the customer receives funds, and know that this corresponds to the information previously collected about the customer. It is also important that the obliged entity knows and is convinced that the customer's activities and circumstances do not refer to money laundering or terrorist financing or transactions that are unusual in any other respect.

Customer principle[57]. Upon compliance with the Know-Your-Customer principle, the objective of the obliged entity is to understand what service the customer wants to get and for what purpose, i.e. does this request correspond to the customer's actual activities, capability and needs, and the customer's knowledge and understanding of the specifics, nature, etc. of the customer's business activities. The scope of knowing the customer must correspond to the results of the risk assessment of the obliged entity (see point 3.3 of these Guidelines) and the risk associated with the customer, i.e. the higher the risk associated with the customer, the more measures the obliged entity must take to understand the customer and their activities. All in all, the purpose is to understand and identify the risk profile associated with the customer and the business relationship. On the basis of the collected information, the obliged entity can assess what the expected future activities of the customer will be like and thereby monitor the business relationship and assess the activities of the customer against the information already collected. Thus, the regime of future monitoring of the business relationship is defined on the basis of the risk profile as a due diligence measure applied to the customer. It is thereby important that the obliged entity knows and is convinced that the customer's activities and circumstances do not refer to money laundering or terrorist financing or transactions that are unusual in any other respect.

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

4.1.5. Upon the monitoring of the business relationship

4.1.5.1. the due diligence measures taken are:

i. checking of transactions made in a business relationship in order ensure that the transactions correspond to the obliged entity's knowledge of the customer, their activities and risk profile (see point 4.4.1 of these Guidelines);

ii. regular updating of relevant documents, data or information gathered in the course of application of due diligence measures (see point 4.4.2 of these Guidelines);

iii. identification of the source and origin of the funds used in a transaction (see point 4.4.3 of these Guidelines).

4.1.5.2. The purpose of application of due diligence measures is to assess and ensure that the transactions carried out during the business relationship and the customer's activities in general correspond to the information collected in the course of the implementation of the Know-Your-Customer principle upon the establishment of the business relationship. This way, the obliged entity assesses and knows the purpose for which and the economic or legal relationship within the scope of which the customer concludes transactions or receives funds during the business relationship and knows that this corresponds to the information previously collected. It is thereby important that the obliged entity knows and is convinced that the customer's activities and circumstances do not refer to money laundering or terrorist financing or transactions that are unusual in any other respect.

[57] In English – Know-Your-Customer aka KYC.

4.1.6. The obliged entity must apply all due diligence measures[58], i.e. they may not leave any due diligence measures unapplied in any stage, but they may choose the scope of application of due diligence measures according to the risk associated with the customer and the business relationship between the customer and the obliged entity. This means that due diligence measures are applied on a risk basis[59] and that upon the application of due diligence measures, the obliged entity proceeds from the principles that suit their business strategy and implements them to the extent that corresponds to their prior risk assessment. If a risk related to a customer or the person of the customer participating in a transaction has been determined as low, the obliged entity may apply simplified due diligence measures, but not applying due diligence measures at all is not permitted. Measures must be applied to a larger extent, i.e. by enhanced procedure, if the risk arising from the customer or the person participating in the transaction is higher than usual.

4.1.7. Due diligence measures must be applied:

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

4.1.7.2. upon executing or mediating occasional transactions outside a business relationship where the value of the transaction exceeds 15,000 euros or an equal amount in another currency[60], regardless of whether the financial obligation is performed in the transaction in a lump sum or in several linked payments over a period of up to one year, unless otherwise provided by law. Due diligence measures must thereby be applied as soon as the exceeding of the sum becomes known or, where the exceeding of the sum depends on the making of several linked payments, as soon as the sum is exceeded;

4.1.7.3. upon verification of information gathered while applying due diligence measures or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered earlier while updating the relevant data;

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

4.1.8. Due diligence measures must not be applied in circumstances where the situation specified in point 4.1.7 has not occurred. However, the payment service provider of the payer and the payee must identify the customer in the case of every transfer of funds[61] where the sum of the financial obligation exceeds 1,000 euros, regardless of whether the financial obligation is performed in a lump sum or in several linked payments over a period of up to one month. Here, identity must also be ascertained as soon as the exceeding of the sum becomes known or, where the exceeding of the sum depends on the making of several linked payments, as soon as the sum is exceeded.

4.1.9. Proceeding from the above, the primary requirement of the measures of money laundering and terrorist financing prevention is that the obliged entity not enter into transactions or establish relationships with anonymous or unidentified persons. Legislation stipulates the obligation of the obliged entity to refuse to conclude a transaction or establish a business relationship if the person does not submit as much information as required for their identification or about the objectives of

[58] Excl. the case stipulated in point 4.8.3 of these Guidelines.
[59] See also point 4.2 of these Guidelines.
[60] The obliged entity thereby assesses the situations where a person participating in an occasional transaction knowingly or in a manner that refers to such activities concludes transactions once or several times in sums smaller than 15,000 euros and takes into account that such transactions may refer to suspicious or unusual transactions, which is why the obliged entity must perform additional obligations (incl. refusal to conclude the transaction and the obligation to report to the Financial Intelligence Unit).
[61] The transfer of funds is defined in point (9) of Article 3 of Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (OJ L 141, 5.6.2015, p. 1–18).

transactions or if their activities create suspicions of money laundering or terrorist financing (see also point 6.1 of these Guidelines). In certain cases, the obliged entity is obliged to exercise their right and refuse the transactions concluded within the scope of the business relationship (see also point 6.2 of these Guidelines). Legislation also stipulates the obligation of the obliged entities to terminate a long-term contract without notice if the person does not submit sufficient information for the application of due diligence measures (see also point 6.3 of these Guidelines).

4.1.10. Upon the application of any due diligence measure, the obliged entity takes into account the money laundering and terrorist financing risks and methods specific to Estonia given in Annexes 1 and 2 to these Guidelines.

4.1.11. The application of due diligence measures is a duty assigned to the obliged entity. Due diligence measures cannot be left unapplied for the reason that another credit or financial institution should have implemented due diligence measures for the same customer or their transactions[62].

4.1.12. The information and data collected in the course of the application of due diligence measures and the measures taken for the prevention of money laundering and terrorist financing must be retained (see point 5 of these Guidelines).

4.1.13. The management board of the obliged entity must ensure compliance with due diligence according to the recommendations made in these Guidelines, and consider that the implemented measures are appropriate, correspond to the activity profile of the service provider and are in accordance with the nature and scope of the customers and the transactions as well as the associated money laundering and terrorist financing risks.

4.2. Risk-based approach upon the application of due diligence measures

4.2.1. The obliged entity must recognise, understand and assess the risks related to money laundering and terrorist financing in their own activities and the activities of their customers (incl. the risks that emerge before the application of countermeasures). In this manner, the obliged entity assesses, in the case of the risk-based approach, the probability of the realisation of the risks and the consequence of their realisation. Upon the assessment of probability, the possibility of the emergence of the respective circumstances must be taken into account, i.e. the possible threats must be assessed, which may affect the activities of the customer or the obliged entity and the possibility that the probability of the emergence of the given threat will increase.

4.2.2. Upon the assessment of the specific risks related to the customer and the separate business relationship or a person participating in an occasional transaction, the obliged entity identifies the risk profile of the customer or the person participating in the transaction and determines the risk level in confluence with the risk profile associated with the business relationship and the risk level (hereinafter jointly the *risk profile and risk level*) at least on the scale of lower than average (low), average and higher than average (high).

4.2.3. Determination of the risk level means that the obliged entity considers the activities or actions not expected from certain customers or business relationships to be possible[63], which is why more attention must constantly be paid to the customer and their activities. Or vice versa, the obliged entity does not consider such activities possible from certain customers, which is why the extent of giving attention is different. Determining a risk level that is higher than usual does not mean that the customer launders money or finances terrorism but that more attention must be given to the customer's activities and the circumstances associated with them when considering the

[62] For example, if a payment is received from another credit or financial institution, this does not release the obliged entity from the obligation to identify the source and origin of the funds used in the transaction.
[63] Considering primarily the nature, scope and level of complexity of their services, incl. the risk appetite and risks arising from activities of the obliged entity.

circumstances as a set. Neither does determining a lower risk level mean that the customer cannot be associated with money laundering or terrorist financing.

4.2.4. In order to determine the risk profile and risk level, the obliged entity takes into account:

4.2.4.1. the risk assessment prepared on the basis of point 3.3 of these Guidelines;

4.2.4.2. the purpose of the business relationship or the occasional transaction and the information that the obliged entity has collected about the objective of the business relationship or the occasional transaction within the meaning of point 4.3.6 of these Guidelines, considering the factors specified in Annexes 1 and 2 to these Guidelines;

4.2.4.3. the volume of the assets deposited by the customer or the value of an occasional transaction;

4.2.4.4. the expected duration of the business relationship;

4.2.4.5. primarily the provisions of §§ 34 and 35 of the MLTFPA as circumstances characterising lower risk and the provisions of §§ 37, 39, 40 and 41 of the MLTFPA as circumstances characterising higher risk;

4.2.4.6. the relevant guidelines and instructions of European Union organisations, the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism of the Council of Europe Moneyval, FATF and the European Supervisory Authorities (the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA)); and

4.2.4.7. primarily the guidelines of the European Banking Authority (EBA) (incl. the risk factors specified therein), which describe the simplified and enhanced due diligence measures applied to customers and the factors that credit and financial institutions should take into account when they assess the risk of money laundering and terrorist financing associated with single business relationships and occasional transactions (hereafter *Guidelines on Risk Factors*)[64].

4.2.5. The obliged entity assesses the meaning of the risk profile of the customer and the business relationship and the various risk factors, and the impact they have on the determination of one or another risk level. Upon the determination of the risk level, it must be kept in mind that:

4.2.5.1. the determination or consideration of the risk level may not be impermissibly influenced by just one risk factor, unless the risk factor independently does not call for the determination of a high risk level (e.g. the status of a high-risk politically exposed person, etc.);

4.2.5.2. the weight of risk factors may not be influenced by the economic or profit-related considerations of the obliged entity;

4.2.5.3. the methodology used to determine the risk level may not unreasonably lead to the situation where no business relationships can be classified as high-risk business relationships;

4.2.5.4. the methodology used to determine the risk level may not unreasonably lead to the situation where the risk level of most customer relationships is lower than usual; and

[64] Guidelines on Risk Factors. Online: https://www.fi.ee/public/pp_nr_10_Guidelines_on_Risk_Factors_ET_04-01-2018.pdf. (19.11.2018)

4.2.5.5. consideration of the risk factors of the customer may not be in conflict with the relevant directives of the European Parliament and of the Council[65], the MLTFPA or these Guidelines, which describe the situations that always refer to a higher risk/threat of money laundering or terrorist financing.

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

4.2.6.1. the customer or the beneficial owner is a high-risk politically exposed person (see also point 4.3.4 of these Guidelines);

4.2.6.2. the obliged entity establishes a correspondent relationship with a high-risk or third country respondent institution (see also point 4.9 of these Guidelines);

4.2.6.3. the obliged entity deals with or provides services to natural persons or legal entities that originate from a high-risk or non-cooperating country entered in the FATF list, a high-risk third country or a higher risk[66] country or territory or they have the citizenship of such a country or their place of residence or location or the location of the payee's payment service provider is in such a country or territory (see also point 4.10 of these Guidelines);

4.2.6.4. transactions are related to complicated, high-value and unusual transactions and transaction patterns without any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question (see also points 4.4.2 and 4.6.6.2 of these Guidelines);

4.2.6.5. several of the circumstances referring to the risks highlighted in Annexes 1 and 2 to these Guidelines are present at the same time.

4.2.7. In order to identify the risk factors specified in point 4.2.4.7 of these Guidelines, the obliged entity applies additional due diligence measures if necessary, incl. the additional measures related to the identification of the objective of the business relationship or the occasional transaction (see also point 4.3.6 of these Guidelines).

4.2.8. The obliged entity applies measures, incl. enhanced due diligence measures in appropriate cases, within the meaning of point 4.6 of these Guidelines in order to mitigate the specific risks identified in respect of a customer. This means that the obliged entity directs their resources to the place where these are the most necessary and important.

4.2.9. Every time when automatically assigned risk levels must be reassessed, the reasons of the reassessment must be appropriately documented.

4.2.10. The manual reduction of a risk level from higher than usual to average is possible, but this is only done in the case of justified circumstances and considering, among others, the circumstance why giving additional attention to the customer or their activities is no longer necessary. When the risk

[65] The relevant directive of the European Parliament and of the Council within the meaning of these Guidelines is the European Union directive concerning the prevention of money laundering and terrorist financing effective in the European Union at the moment the obligation is performed.

[66] Higher risk countries and jurisdictions are, among others, those:
1) that, according to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, have not established effective AML/CFT systems;
2) that, according to credible sources, have significant levels of corruption or other criminal activity;
3) that are subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
4) that provide funding or support for terrorist activities, or that have designated terrorist organisations operating within their territory, as identified by the European Union or the United Nations;
5) that the obliged entity itself defines as higher risk countries.

level is changed in such a manner, the obliged entity must be prepared to explain (incl. to Finantsinspektsioon), if necessary, why the risks identified earlier are no longer relevant and why reducing the risk level is justified. The fact that the customer has not concluded transactions referring to the risk that is higher than usual over a certain period of time or has not concluded transactions that the obliged entity considered possible upon the determination of a higher risk level does not mean that the customer will not conclude such transactions or perform such actions in the future or that the features and circumstances referring to a higher risk level have been overcome/disappeared, etc.

4.2.11. The obliged entity must document the determination of the risk level (e.g. in a single database), update it and make these data and reasons accessible to competent authorities as necessary.

4.3. Due diligence measures upon the establishment of business relationships

4.3.1. Identification of a natural person, representative and civil law partnership

General principles

4.3.1.1. Upon the establishment of a business relationship or the completion of an occasional transaction or in the case specified in point 4.1.8 of these Guidelines, the obliged entity must identify the natural person who is the customer or the person participating in an occasional transaction and verify the submitted information on the basis of the information obtained from a reliable and independent source.

4.3.1.2. The obliged entity must ascertain whether the person is acting on behalf of themselves or another person (natural person or legal entity). If the person acts on behalf of another person, the obliged entity must also implement the measures specified in point 4.3.1.28 of these Guidelines in respect of the person on whose behalf transactions are concluded (see also the identification of legal entities in point 4.3.2 of these Guidelines).

4.3.1.3. If the customer or the person participating in an occasional transaction has a representative, the representative must be identified and the submitted information must be verified on the basis of the information obtained from a reliable and independent source. In this manner, all of the requirements for identification and verification of customers specified in point 4.3.1 apply to the identification and verification of the representative. The requirements arising from points 4.3.1.24 to 4.3.1.27 of these Guidelines also apply here.

4.3.1.4. For a payment service provider that performs transactions outside a business relationship, the identification and verification obligation within the meaning of point 4.1.8 of these Guidelines arises in respect of the payer as well as the payee (the latter applies if the payee uses the payment service provider for the purpose of collecting funds (is the payee's payment service provider)).

4.3.1.5. In the case of persons with restricted active legal capacity, incl. minors, the obliged entity must also proceed from the provisions of the General Part of the Civil Code Act, the Law of Obligations Act and the Family Law Act in addition to the instructions given in these Guidelines and the MLTFPA. In addition to the personal data of the person with restricted active legal capacity, the personal data of the legal representative (parent(s) or guardian(s)) must also be verified upon identification.

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

4.3.1.7. The obliged entity must not identify and verify a natural person again if they already have an effective business relationship with the same natural person and the same natural person wants to enter into a new long-term contract or receive a new financial service[67]. The above also applies if a natural person who has been identified and verified within the scope of another legal relationship, in which the person was the representative of another customer, wants to establish a new business relationship[68]. The above also applies on the assumption that the obliged entity has no suspicions about the authenticity and validity of the data concerning the customer at the moment of emergence of the identification obligation (incl. the data collected in the course of the identification of the customer and the beneficial owner). The above does not mean that the purpose of a new business relationship should not be identified in the case of the customer within the meaning of point 4.3.6 of these Guidelines or that the business relationship should not be monitored within the meaning of point 4.4 of these Guidelines. Using the exception described in this point, the customer file (i.e. the place where the data collected in the course of due diligence measures are retained) must include a clear reference to the place where the documents collected in the course of identification can be accessed (i.e. the customer file where the data collected in the course of the initial identification are retained).

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

Time of identification

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

Identification

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

i. the person's name;

ii. the person's personal identification code, or if the person doesn't have one, their date and place of birth and place of residence or location,

as well as other data directly related to the person, such as:

iii. place of residence[69];

[67] In the case of the thresholds specified in point 4.3.1.14 of these Guidelines, the total amount of all such outgoing payments must be cumulatively taken into account.

[68] Said exception does not apply to persons who have been identified and verified in a situation where they were the beneficial owner of another customer.

[69] The address registered in the Population Register or another similar register is not important in the case of the place of residence, but the place where the person permanently or mainly resides is important. The person's habitual residence must be ascertained if ascertaining a person's permanent place of residence is difficult (e.g. the person's place of residence cannot be ascertained or they have several places of residence). A PO Box number or *poste restante* address cannot be regarded as the

iv. profession or area of activity, if necessary[70].

4.3.1.11. The following documents are used for identification:

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

ii. a valid travel document issued in a foreign country;

iii. a driving licence that complies with the conditions stipulated in subsection 4 (1) of the Identity Documents Act;

iv. in the case of a person under seven (7) years of age, the birth certificate specified in § 30 of the Vital Statistics Registration Act; or

v. a copy of the aforementioned documents that has been authenticated by a notary, certified by a notary or officially[71] certified.

4.3.1.12. Upon the demand of the obliged entity, the customer submits the documents and provides the information required for identification. Upon the demand of the obliged entity, the customer confirms with their signature that the information and documents submitted for the application of the due diligence measures are true.

Verification of the information obtained in the course of identification and manner of verification

4.3.1.13. Verification of the information obtained in the course of identification means using data from a reliable and independent source to confirm that the data specified in point 4.3.1.10 of these Guidelines are true and correct (first two sub-points)[72], also confirming, if necessary, that the data directly related to the person (third and fourth sub-point) are true and correct. This means that the purpose of verification of information is to obtain reassurance that the person who wants to establish a business relationship or conclude an occasional transaction is the person they claim to be.

4.3.1.14. Verification of information collected in the course of identification of a person[73]:

i. must be carried out face-to-face or with an IT device (i.e. video identification) if the total amount of the outgoing payments per calendar month exceeds 15,000 euros in the case of a natural person and 25,000 euros in the case of a legal entity, irrespective of the person's origin or their place of residence or location;

---

habitual residence. Habitual residence is the place where the person wants to be and to which they are connected. A person's habitual residence is not just the place where the person 'permanently or mainly' resides; the intentions and future plans of the person in relation to staying in the specific country or place are also important when the habitual residence is determined. This is an autonomous term and therefore does not depend on the national substantive law. The place of residence is important for the identification of the purpose and nature of the business relationship as well as the updating of the customer's data during the further monitoring of the business relationship.

[70] Asking about the profession or area of activity is not an imperative obligation or something that must always be done, but it may be important for the identification of the objective of the business relationship (in the confluence of clause 20 (1) 4) and subsection 20 (2) of the MLTFPA), verification of the data obtained in the course of identification (whether the person who wants to establish a business relationship or conclude an occasional transaction is the person that they claim to be) as well as identification of the status of a politically exposed person (does the person work in the position of a politically exposed person).

[71] In the case of an officially certified copy, the obliged entity assesses whether the rights of the person who certified the copy extended to the certification of the copy of the document.

[72] For example, queries that confirm the validity of a document without showing to whom the document belongs and what other data are related to the person do not make it possible to verify information.

[73] A 'person' within the meaning of this point is a customer who is a natural person or in the case of a legal entity the representative of the customer, who is identified.

ii. must therefore not be carried out face-to-face or with an IT device (i.e. video identification) and the possibility stipulated in point 4.3.1.18 of these Guidelines (two sources) can be used instead if (i) the total amount of the outgoing payments per calendar month is less than 15,000 euros in the case of a natural person and less than 25,000 euros in the case of a legal entity; and (ii) the person is from a contracting state of the European Economic Area or their place of residence or location is there.

4.3.1.15. Face-to-face identification means that the customer or their representative and the representative of the obliged entity are in the same place within the scope of a specific meeting. This means that the potential customer or their representative has direct contact with the representatives of the obliged entity in the course of which the obliged entity observes point 4.3.1.13 of these Guidelines by comparing the person's biometrics (facial image) with the facial image on or obtained from the document[74] specified in point 4.3.1.11 of these Guidelines. Direct contact requires direct communication between the representative of the obliged entity and the customer or their representative to assess the compliance of the content of their declaration of intent and goal with the actual intent. The experience obtained in the course of the direct contact makes it possible to determine the customer's risk level more accurately. The contact may take place outside the permanent place of business of the obliged entity if at least the same due diligence obligations that are performed in ordinary cases are performed in its course.

4.3.1.16. In the case of identification with an IT device, the obliged entity complies with the requirements stipulated in § 31 of the MLTFPA and the technical requirements and procedure specified in the regulation of the Minister of Finance established on the basis of the authorisation provision stipulated in subsection (6) of the same section. The objective, among others, is to compare the person's biometrics (facial image) obtained in the course of the session with the facial image on or obtained from the document[75] specified in point 4.3.1.11 of these Guidelines.

Reliable and independent source

4.3.1.17. The (i) face-to-face identification[76] or (ii) identification with an IT device[77] or (iii) identification on the basis of the copy of an identity document authenticated by a notary or certified by a notary or officially certified and when seeing the original of the copy in respect of the person specified in point 4.3.1.14 of these Guidelines is deemed to be the reliable and independent verification of the information obtained in the course of identification because an identity document that is valid and issued by an independent state authority is seen during this.

4.3.1.18. In situations not specified in point 4.3.1.17 of these Guidelines, the reliable and independent source (must exist cumulatively) is verification of the information obtained in the course of identification, (a) which originates from two different sources, (b) where, if the money laundering and terrorist financing risk of the customer and the business relationship is average or higher than usual, the customer sends a photo taken of the facial image of the person for the specific financial service immediately before the data are sent and the obliged entity makes

[74] In certain cases, it is possible to obtain the person's facial image from the databases of the relevant reliable and independent competent authorities (such as the Police and Border Guard Board when the number of the person's identity document is known).
[75] In certain cases, it is possible to obtain the person's facial image from the databases of the relevant reliable and independent competent authorities (such as the Police and Border Guard Board when the number of the person's identity document is known).
[76] See also point 4.3.1.15 of these Guidelines.
[77] See also point 4.3.1.16 of these Guidelines.

sure that the photo was taken recently[78] and (c) which corresponds to the following features, i.e. reliable and independent source is information:

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

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

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

4.3.1.19. Irrespective of the selected reliable and independent source, the obliged entity must make sure in the case of identity documents that (i) the document is valid and complies with the requirements stipulated in the Identity Documents Act and (ii) the person resembles the person depicted on the document photo in terms of appearance and age and the data included in the document[79].

4.3.1.20. When obtaining reliable and independent information, the obliged entity must ensure, especially in the case stipulated in point 4.3.1.18 of these Guidelines, that the obtained reliable and independent information is not so-called black and white and/or illegible copy.

4.3.1.21. The obliged entity assesses in which cases the manner of forwarding the reliable and independent source or obtaining this source must also be a reliable and independent channel or measure, considering the risk-based approach, i.e. the risk associated with the customer and the business relationship and their risk profile, when making such an assessment.

Two different sources

4.3.1.22. One of the sources is always:

i. an identity document with a photo stipulated in point 4.3.1.11 of these Guidelines or a coloured and legible copy/image of this document; or

ii. data and a photo of the person on the same document obtained from reliable and independent sources[80]; or

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

[78] The obligation in point (b) must not be complied with if the money laundering and terrorist financing risk associated with the customer and the business relationship is lower than usual.
[79] Point (ii) is not applied if the obliged entity verifies the data collected in the course of identification from two sources and the first mandatory source within the meaning of point 4.3.1.22 of these Guidelines is the information (at least the name and personal identification code or the date and place of birth if there is no personal identification code) obtained in the course of strong authentication carried out with a digital personal identification tool if the money laundering and terrorist financing risk associated with the customer and the business relationship is lower than usual, and the audit trail proving that this was done (i.e. the first mandatory source is the one specified in sub-point 3 of point 4.3.1.22 of these Guidelines).
[80] For example, a document photo obtained from the Police and Border Guard Board.

authentication[81] carried out with a digital personal identification tool if the money laundering and terrorist financing risk associated with the customer and the business relationship is lower than usual, and the audit trail proving that this was done.

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

i. another document that complies with the conditions in sub-points 1 or 2 of point 4.3.1.22 of these Guidelines (a copy thereof or the data and photo obtained therefrom); or

ii. the information (at least the name and personal identification code or the date and place of birth if there is no personal identification code) obtained in the course of strong authentication[82] carried out with a digital personal identification tool and the audit trail proving that this was done [83]; or

iii. verification of the data directly related to a person via the Population Register[84] or an equivalent register, provided that the source is a reliable and independent source within the meaning of point 4.3.1.18 of these Guidelines; or

iv. information received from a firstpayment[85]; or

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

vi. information for checking the data directly associated with the person (e.g. place of work, residence or study)[86].

Differences in the case of representation

4.3.1.24. In the case of representation, the obliged entity must also identify and verify the nature and scope of the right of representation. If the right of representation does not arise from law, the name, date of issue and name of issuer of the document that serves as a basis for the right of representation must be ascertained and retained[87].

4.3.1.25. The representative of a foreign legal entity must submit, on the request of the obliged entity, a document that proves their authorisation and has been certified by a notary or in an equivalent manner and that has been legalised or certified with a certificate that replaces legalisation (Apostille)[88], unless otherwise stipulated in the international agreement.

---

[81] Strong authentication is authentication that is based on the use of at least two security elements that function independently and guarantee the confidentiality of the authentication data, that are known to or owned only by the customer or that can only be ascribed to the customer. A personalised security element is a component that has been connected to a person and can be used for authentication.

[82] *Ibid*.

[83] Such a document may also be the identity document that was used in the performance of the obligation stipulated in sub-point 1 of point 4.3.1.22 of these Guidelines. Upon the implementation of sub-point 3 of point 4.3.1.22 of these Guidelines, strong authentication can only be used with another digital identification tool that allows for strong authentication.

[84] Legal entities and natural persons may access the Population Register in the case of legitimate interest.

[85] This means that the customer or a person participating in the transaction makes a transfer to the obliged entity's account from a bank account or payment account that belongs to them and has been opened in a credit or payment institution that implements requirements equal to those established in the relevant directives of the European Parliament and of the Council.

[86] For example, the fact that the data collected in the course of identification are true and correct can be proven by a confirmation in a format that can be reproduced in writing received from a reliable and independent source, which states that the person lives (e.g. consumes utilities there, i.e. proves that the person lives at that place), studies or works (profession or area of activity) at the place they declared, etc.

[87] When a document including the right of representation is handled, it must also be ascertained whether the persons who issued it had the relevant competency.

[88] See point 4.3.2.15 of these Guidelines for legalisation and Apostille.

4.3.1.26. When the right of representation of authorised and legal representatives is handled, it must be ascertained whether the representative knows their customer[89]. In order to ascertain the nature of the actual relationships between the representative and the represented person, the representative must know the content and objective of the declarations of intent of the person they represent, and they must also be able to answer other relevant questions about the represented person's location, areas of activity, turnover and transaction partners, other related persons and beneficial owners. The representative must also confirm that they are aware of and convinced about the source and legal origin of the funds used by the represented person in the transaction.

4.3.1.27. The obliged entity must observe the conditions of the right of representation granted to the representatives and provide services only within the scope of the right of representation (e.g. is the transaction a one-off or a series of repeated transactions over a certain period of time).

Beneficial owner of a natural person

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

4.3.1.29. If the obliged entity ascertains that transactions or actions are actually performed on behalf of a third party, and the content of the activities suggests the possible activities of a trust, the obliged entity must take all measures to identify the beneficial owner of the trust within the meaning of point 4.3.3 of these Guidelines and perform all actions to ascertain the actual purpose of the business relationship within the meaning of point 4.3.6 of these Guidelines. For the purposes of the General Part of the Civil Code Act, this may mean that a business relationship with such a trust[90] cannot be established, as the person who actually wants to establish the business relationship or perform the act is a trust[91] that does not have legal capacity pursuant to Estonian law.

Differences in the case of civil law partnerships

4.3.1.30. The objective of identification of civil law partnerships[92] is to identify all members of the civil partnership or their representatives on the same basis applied to customers who are natural persons. The beneficial owners of the civil law partnership must be identified according to point 4.3.3 of these Guidelines and the objective of the business relationship or an occasional transaction must be ascertained according to point 4.3.6 of these Guidelines.

4.3.1.31. In other respects, all of the due diligence measures, data retention obligations and the obligation to report to the Financial Intelligence Unit that are applied to customers or persons concluding occasional transactions also apply to civil law partnerships.

Data retention

[89] A person representing a legal entity is expected to know the entity's economic and professional activity, i.e. the area of activity, the objectives of their transactions, payment practices, experience, activity partners, source and origin of the funds used in transactions, owners, etc.
[90] The given term in English – trust.
[91] *Ibid*.
[92] See § 580 et seq. of the Law of Obligations Act about the legal nature of civil law partnerships.

4.3.1.32. The information and documents concerning identification are retained on the basis of clause 5 of these Guidelines.

4.3.2. Identification of a legal entity

General principles

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

4.3.2.2. The representative of a legal entity is identified and the obtained data are verified on the basis of point 4.3.1 of these Guidelines.

4.3.2.3. The obliged entity must not identify and verify a legal entity and their representative and beneficial owners again if they already have an effective business relationship with the same legal entity and the same legal entity wants to enter into a new long-term contract or receive a new financial service[93]. The above also applies if a natural person who has been identified and verified within the scope of another legal relationship, in which the person was the representative of another customer, wants to establish a new business relationship[94]. The above also applies on the assumption that the obliged entity has no suspicions about the authenticity and validity of the data concerning the customer (incl. the data collected in the course of the identification of the customer and the beneficial owner). The above does not mean that the purpose of a new business relationship should not be identified in the case of the customer within the meaning of point 4.3.6 of these Guidelines or that the business relationship should not be monitored within the meaning of point 4.4 of these Guidelines. Using the exception described in this point, the customer file (i.e. the place where the data collected in the course of due diligence measures are retained) must include a clear reference to the place where the documents collected in the course of identification can be accessed (i.e. the customer file where the data collected in the course of the initial identification are retained).

4.3.2.4. The obliged entity is prepared, if necessary, to explain the selection of the identification measure and the verification measure to Finantsinspektsioon, incl. demonstrate why the information is from a reliable and independent source, what the two different sources are and justify why the selected measure complies with the risk profile and risk level of the customer and the business relationship with the customer.

Time of identification

4.3.2.5. The obliged entity must identify the customer and verify the identification data within reasonable time before the initiation of the actions related to the entry into a long-term contract or at the time of entry into such a contract. A person who participates in a transaction must be identified before the commencement of the acts of completing the transaction or during the completion of the transactions.

Identification

[93] In the case of the thresholds specified in point 4.3.1.14 of these Guidelines, the total amount of all such outgoing payments must be cumulatively taken into account.

[94] Said exception does not apply to persons who have been identified and verified in a situation where they were the beneficial owner of another customer.

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

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

ii. registry code or registration number and date;

iii. name of the director or names of members of the management board or members of another equivalent body, and their authorities in representing the legal entity, whereby the representative who wants to establish a customer relationship is identified and the obtained data are verified according to the requirements of point 4.3.1 of these Guidelines;

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

i. location of the legal entity, whereby the theory of the country of establishment[95] must be proceeded from;

ii. place of business of the legal entity[96];

iii. data of the means of communication of the legal entity.

4.3.2.7. The following documents are used for identification:

i. registry card of the relevant register;

ii. registration certificate of the relevant register; or

iii. a document equivalent with an aforementioned document or relevant document of establishment[97] of the legal entity.

4.3.2.8. Upon the demand of the obliged entity, the customer submits the documents and provides the information required for identification. Upon the demand of the obliged entity, the customer confirms with their signature that the information and documents submitted for the application of the due diligence measures are true. If the obliged entity has access to the relevant registers, they do not have to ask the customer to provide the relevant documents used for identification.

Verification of the information obtained in the course of identification

4.3.2.9. Verification of the information obtained in the course of identification means using data from a reliable and independent source to confirm that the data specified in point 4.3.2.6 of these Guidelines are true and correct (first three sub-points), also confirming[98] that the data directly related to the person (fourth to sixth sub-point) are true and correct. This means that the purpose of verification of information is to obtain reassurance that the person who wants to establish a business relationship or conclude an occasional transaction is the person they claim

[95] According to the theory of country of establishment, the location of a legal entity is the country in which the legal entity was established.

[96] This is determined on the basis of factual circumstances and it is the place where the legal entity operates permanently or primarily and with which the legal entity can be associated with the most – the location of the majority of employees, warehouses and office premises, the place where production takes place or the service is actually provided, etc.

[97] In the case of a foreign legal entity, these are, among others, a certificate of incorporation, certificate of good standing, partnership agreement, deed of trust, memorandum and articles of association of a company, etc.

[98] For example, queries that confirm the validity of a document without showing to whom the document belongs and what other data are related to the person do not make it possible to verify information.

to be.

Reliable and independent source

4.3.2.10. A source is deemed to be reliable and independent if the obliged entity:

i. sees the original of the document specified in point 4.3.2.7 of these Guidelines;

ii. sees a copy of the document specified in point 4.3.2.7 of these Guidelines that has been authenticated by a notary, certified by a notary or officially[99] certified;

iii. has access to the data in the Commercial Register, Register of Non-profit Associations and Foundations or the relevant registers of foreign countries via a computer network.

4.3.2.11. The documents issued by the registers may not have been issued earlier than six months before their submission to the obliged entity. This also applies if a copy has been made of the document.

4.3.2.12. In situations not specified in point 4.3.2.10 of these Guidelines, the reliable and independent source is the verification of the information obtained in the course of identification, which (a) originates from two separate sources and (b) complies with the requirements specified in condition c of point 4.3.1.18 of these Guidelines. However, the provisions of point 4.3.2.10 of these Guidelines must be applied in situations where the representative of a legal entity must be identified face-to-face according to point 4.3.1.14 of these Guidelines.

Two different sources

4.3.2.13. Within the meaning of point 4.3.2.12 of these Guidelines, two different sources means that the data medium, place or measure of obtaining information must be different (i.e. it cannot be the same data medium).

4.3.2.14. In addition to the document[100] specified in point 4.3.2.7 of these Guidelines (if the obliged entity does not select two different identity documents of the customer for verification), the second source may also be information obtained from a reliable and independent source for checking the data directly related to the person (such as the location, etc.).

Legalisation and Apostille, language of documents

4.3.2.15. Public[101] documents issued in a foreign country must be legalised or confirmed with a certificate (an Apostille)[102], i.e. an internationally recognised official certification of the authenticity of the document has been issued for use of an official document issued in one country in another country, whilst legalisation and the attachment of an Apostille does not confirm that the information in the document is true.

---

[99] In the case of an officially certified copy, the obliged entity assesses whether the rights of the person who certified the copy extended to the certification of the copy of the document.

[100] This document must always be one of the two sources.

[101] A public document means an extract from a register, an administrative document (diploma, certificate, statement, notification, etc.), a document issued by a court or an authority related to a court (copy of a court judgment, extract from register, document of a bailiff, etc.) and a document of a notary or a sworn translator.

[102] Apostilles are provided according to the Hague Convention of 5 October 1961: Abolishing the Requirement of Legalisation for Foreign Public Documents (hereinafter the Convention). The states that have joined the Convention have abandoned the complicated process of legislation and replaced it with the simpler Apostille process. The list of states that have joined the Hague Convention can be found on the Hague Conventions' website (see www.hcch.net). The documents that have reached Estonia from these countries must be certified with an Apostille by the relevant authority in the foreign state, which confirms that they have been issued by a competent official.

4.3.2.16. A document must be legalised if it is not subject to confirmation with an Apostille. For legalisation, a document must pass the legalisation authorities of the issuing country and the receiving country of the document[103] (usually ministries of foreign affairs).

4.3.2.17. At the same time:

i. public documents prepared or certified in countries with whom Estonia has entered into the relevant legal assistance agreement[104] do not require legalisation or an Apostille;

ii. legalisation or an Apostille is not required for public documents issued in a country that implements the Convention Abolishing the Legalisation of Documents in the Member States of the European Communities[105].

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

Data retention

4.3.2.19. The information and documents concerning identification are retained on the basis of clause 5 of these Guidelines.

4.3.3. Identification of the beneficial owner of a legal entity

General principles

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

4.3.3.2. The beneficial owner means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or exercises control in another manner[106] over a transaction, act, action, operation or step or over another person and/or in whose interests or for whose benefit or on whose account a transaction or act, action, operation or step is made.

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

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

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

[103] Further information about legalisation can be obtained from the website of the Estonian Ministry of Foreign Affairs (see http://www.vm.ee/?q=taxonomy/term/39). Documents issued in Estonia are also legalised in the Ministry of Foreign Affairs.
[104] At the moment of issue of these Guidelines, such countries are Lithuania, Latvia, Poland, Ukraine and Russia.
[105] At the moment of issue of these Guidelines, such countries are Belgium, Ireland, Italy, Latvia, France and Denmark.
[106] The exercise of control in another manner within the meaning of these Guidelines means the exercise of dominant influence.

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

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

4.3.3.5. The obliged entity must not verify a legal entity and their representative and beneficial owners again if they already have an effective business relationship with the same customer and the same customer wants to enter into a new long-term contract or receive a new financial service. The above also applies on the assumption that the obliged entity has no suspicions about the authenticity and validity of the data concerning the customer (incl. the data collected in the course of the identification of the customer and the beneficial owner). The above does not mean that the purpose of a new business relationship should not be identified in the case of the customer within the meaning of point 4.3.6 of these Guidelines or that the business relationship should not be monitored within the meaning of point 4.4 of these Guidelines. Using the exception described in this point, the customer file (i.e. the place where the data collected in the course of due diligence measures are retained) must include a clear reference to the place where the documents collected in the course of identification can be accessed (i.e. the customer file where the data collected in the course of the initial identification are retained).

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

Identification of the beneficial owner

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

i. is it possible to identify, in respect of the customer that is a legal entity or a person participating in the transaction, the natural person or persons who actually ultimately control the legal entity or exercise influence or control over it in any other manner[107], irrespective of the size of the shares, voting rights or ownership rights or its direct or indirect nature;

ii. whether the customer that is a legal entity or the person participating in the transaction has a natural person or person who owns or controls the legal entity via direct[108] or indirect[109] shareholding. Family connections[110] and contractual connections[111] must also be taken into account here;

[107] These may be situations where control is exercised via personal connections, company financing schemes, or because there are close or intimate family relationships, or historical or contractual relationships, etc. This may also occur in a manner where control is not exercised, but benefits are received from the company.
[108] Direct ownership is a manner of exercising control whereby the natural person owns a 25 percent shareholding plus one share or an ownership right of over 25 percent in the company.
[109] Indirect ownership is a manner of exercising control whereby a 25 percent shareholding plus one share or an ownership right of over 25 percent in the company is owned by a company that is controlled by a natural person or several companies that are controlled by the same natural person.
[110] If persons related via family ties (partners, descendants and ascendants, etc.) seem to be among the owners, it is necessary to check how much of the company belongs to the related persons.
[111] If it seems on the basis of accessible sources or the data submitted by the customer that a person has a bigger shareholding via contractual or other relationships than indicated in the documents, it is necessary determine the size of the shareholding according to the scale of the actual control or influence.

iii. who is the natural person in senior management[112], who must be defined as the beneficial owner, as the answers to the previous two questions have not made it possible for the obliged entity to identify the beneficial owner.

4.3.3.8. A member of senior management specified in point 4.3.3.7 of these Guidelines is a person who:

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

ii. carries out everyday or regular management functions of the company within the scope of executive power (e.g. chief executive officer (CEO), chief financial officer (CFO), director or president, etc.).

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

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

ii. trustee, asset manager or possessor;

iii. person ensuring and controlling the preservation of assets, where such person has been appointed, or

iv. the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.

Verification of data

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

4.3.3.11. In the case of legal entities, this requires, (i) in the case of identifying the purpose and nature of the business relationship, making it possible to conclude that the customer's beneficial owner, if the latter participates actively in the company's activities, is capable of operating in the declared area of activity, with the declared scope of activity and with the declared main business partners and has the required experience[113]; and (ii) that the obliged entity:

i. sees the original of the document specified in point 4.3.2.7 of these Guidelines;

ii. has access to the data in the Commercial Register, Register of Non-profit Associations and Foundations or the relevant registers of foreign countries via a computer network and checks the beneficial owner's data in said register;

iii. sees a copy of the document specified in point 4.3.2.7 of these Guidelines that has been certified by a notary or officially certified;

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

[112] In English – senior management.
[113] See also points 4.3.6.24 to 4.3.6.27 of these Guidelines.

4.3.3.12. If the identity documents of the legal entity or the other submitted documents do not indicate directly who the beneficial owner of the legal entity is, the relevant data (incl. data about being a member of a group and the ownership and management structure of the group) are registered on the basis of the statement of the representative of the legal entity or the document written by hand by the representative of the legal entity. In such a case, the obliged entity must take reasonable measures to verify the submitted information.

4.3.3.13. In the case of a trust, civil law partnership, community or other similar legal entity, conviction must be obtained about the nature of the beneficial owner on the basis of the civil law partnership agreement, letter of wishes, trust deed and other documents in addition to publicly accessible and/or reliable data. The provisions of point 4.3.3.12 of these Guidelines must be applied if the obliged entity wants to use the statement or handwritten document of the beneficial owner.

Identification of ownership and control structure

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

Data retention

4.3.3.15. The obliged entity registers and retains information about all actions undertaken to identify the beneficial owner and the ownership and control structure. The obliged entity also retains all the data found in the course of these actions. The obliged entity does the above on the basis of point 5 of these Guidelines.

4.3.4. Identification of a politically exposed person

General principles

4.3.4.1. Both upon the establishment of a business relationship as well as in the course of a business relationship or if a certain trigger event[114] occurs, the obliged entity will take measures to ascertain whether the customer or the person who wants to conclude an occasional transaction and the beneficial owner or representative of these persons is a politically exposed person (incl. high-risk politically exposed person), their family member or close associate, or if the customer has become such a person.

4.3.4.2. The obliged entity applies the measures specified in point 4.3.4.18 of these Guidelines to high-risk politically exposed persons.

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

High-risk politically exposed person

[114] In English – trigger event.

4.3.4.4. Within the meaning of these Guidelines, a high-risk politically exposed person is any politically exposed person, their family member or close associate, except for a person who is a local politically exposed person, their family member or close associate with a risk that is average or lower than usual[115] (i.e. whose risk is not high).

4.3.4.5. Politically exposed person means at least a natural person who is or who has been entrusted with prominent public functions, incl. a head of State, head of government, minister and deputy or assistant minister; a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors or of the board of a central bank; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a State-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials.

4.3.4.6. The obliged entity has the right to decide to update politically exposed official positions as a result of a risk-based approach and thereby also take additional measures in respect of other official positions. If the state made a similar decision to update official positions as a result of a risk-based approach, the state may require the obliged entity to also take measures in respect of other official positions. In any case, the public functions must be significant and prominent and not associated with persons who are middle-ranking or more junior officials.

4.3.4.7. Local politically exposed person means a person specified in point 4.3.4.5 of these Guidelines, with the exceptions stipulated in point 4.3.4.6 of these Guidelines, who is or who has been entrusted with prominent public functions in Estonia[116].

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

4.3.4.9. In the case of a state-owned customer that is a legal entity or a person concluding an occasional transaction, the person must be considered a politically exposed person if the politically exposed person has a significant and prominent function[117] in the company and the state owns at least 50% of this company. Upon the assessment of such a significant and prominent function, it is necessary to also assess whether the politically exposed person has any (substantial)[118] authorisation over the state's assets or funds or policies or activities, whether they have the right to issue licences or permits, make exceptions, whether they have control or influence over the accounts or funds of the state or the company, etc.

High-risk local politically exposed person

4.3.4.10. Upon defining a high-risk local politically exposed person, the obliged entity considers the provisions of point 4.2 of these Guidelines and especially the provisions of point 4.2.3 and, if necessary, the probability that:

[115] The provisions of point 4.2 of these Guidelines and especially of points 4.2.3 and 4.3.4.10 must be taken into account upon risk assessment.

[116] Until the amendment of clause 3 12) and § 41 of the MLTFPA after the establishment of these Guidelines, the part of the sentence "who performs or has performed significant public functions in Estonia" must be read as "who performs or has performed significant public functions in Estonia, another contracting state of the European Economic Area or an institution of the European Union".

[117] I.e. owns a function that is not associated with middle-ranking or more junior officials.

[118] In English – substantial.

i. the person, their family member or close associate takes advantage of their position as a politically exposed person, incl. carries out acts for personal gain that is in contravention of the activities expected of their position or conceals illegally earned income; and that

ii. this person has significant influence or the possibility and capability to control or direct assets.

4.3.4.11. Such estimate of probability is based on the general knowledge, prior experience or other knowledge of the obliged entity and takes into account the general level of corruption of the state or the specific job or position, length of service in the position, the obligation to submit a declaration of economic interests associated with the position, the possible links between the specific job or position and economic sectors that may be related to corruption, the existence of negative information about the person, etc. The obliged entity must also consider the other indicators arising from the risk-based approach described in point 4.2 of these Guidelines, which suggest that the risk associated with the customer or the business relationship and their risk profiles is higher than usual.

Family member

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

Close associate

4.3.4.13. A person known to be close associate[119] is:

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

ii. a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person or local politically exposed person;

iii. who is known[120] to have a relationship with the beneficial owner that does not quality as the status of a family member (e.g. boyfriend or girlfriend, mistress, etc.).

Measures taken for identification of a high-risk politically exposed person

4.3.4.14. A high-risk politically exposed person can be identified in the following ways:

i. screening of new, potential and existing customers or persons who want to conclude occasional transactions, their beneficial owners and representatives against the relevant internal or external databases (i.e. name checks in databases[121]) that provide the relevant service;

[119] In English – close associate, i.e. the definition within the meaning of the FATF standards is broader than suggested by the Estonian word 'kaastöötaja' (co-worker).
[120] Known means that this is a fact about which the customer is not and does not have to be asked questions. For example, it is a fact that is known to the general public and also to an average person without them having to read, listen or view specific media.
[121] This must correspond to the fuzzy match principle, i.e. a 100% match of the name is not necessary, and measures must be taken to check matches of less than 100%. The obliged entity must make sure whether this is the same person or not.

ii. asking the representative (covers asking the representative and beneficial owner as well as their family members and close associates) or the person concluding an occasional transaction about the status of a politically exposed person, also asking, where necessary, the customer or the person concluding an occasional transaction about their profession or area of activity and asking the aforementioned data again during the updating of data carried out in the course of the business relationship;

iii. in certain cases, obtaining information about the person from public accessible or third sources in addition to the information specified in the previous point.

4.3.4.15. Sub-point 2 of point 4.3.4.14 of these Guidelines must be applied generally[122] and sub-point 3 must be applied when[123] sub-point 1 is not applied. As a result of the risk-based approach, the obliged entity may also take additional measures in comparison with the measures specified in point 4.3.4.14. Said measures are applied in conjunction with the identification of the purpose and nature of the business relationship or occasional transaction, whereby the obliged entity, upon obtaining inner conviction, may also identify suspicious or unusual circumstances, which may refer to the existence of a politically exposed person or their connection.

4.3.4.16. The measures taken to identify a high-risk politically exposed person must be risk-based, i.e. correspond to the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and risks arising from activities of the obliged entity. This means that the bigger the customer base of the obliged entity and the higher the risk that a business relationship is established with a high-risk politically exposed person and the risk that a high-risk politically exposed person may want to legalise (i.e. launder) criminal proceeds[124] or finance terrorism[125] via the services provided by the obliged entity, the more or the more extensive measures the obliged entity must take from among the measures specified in point 4.3.4.14 of these Guidelines (in conjunction with point 4.3.4.15 of these Guidelines).

4.3.4.17. In any case, the obliged entity is ready to justify to Finantsinspektsioon why the obliged entity did not select the screening of new, potential and existing customers or persons wishing to conclude occasional transactions, and why the circumstances and risks specified in point 4.3.4.16 of these Guidelines are not present.

Measures taken in respect of a high-risk politically exposed person

4.3.4.18. In addition to the general due diligence measures specified in point 4.3 of these Guidelines, the obliged entity applies the following due diligence measures to high-risk politically exposed person:

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

ii. applies measures to establish the source and/or origin of the wealth of the person and the sources of the funds that are used in the business relationship or upon executing

[122] Except if the obliged entity is convinced that the person cannot be a politically exposed person or if the person is a local politically exposed person and it is clear to the obliged entity that the person is not a high-risk local politically exposed person. In such a case the obliged entity may also decide to partially apply the measure specified in sub-point 2 (e.g. only asks about the profession or area of activity). However, the obliged entity is prepared to explain how they knew that the person is not a (high-risk) politically exposed person and why the person was therefore not asked if they are a politically exposed person.
[123] Excl. the cases specified in footnote 122 of these Guidelines.
[124] See also Annex 1 to these Guidelines.
[125] See also Annex 2 to these Guidelines.

occasional transactions;

iii. monitors the business relationship in an enhanced manner within the meaning of point 4.4 of these Guidelines (see also point 4.6 of these Guidelines).

4.3.4.19. Senior management within the meaning of point 4.3.4.18 of these Guidelines and within the meaning of the entire Guidelines is the person who has a sufficiently high position, the right to make decisions and thorough knowledge of the organisation and its capacity in order to make informed decisions in issues directly affecting the company's risk profile and who knows that the compensation mechanisms of the obliged entity are adequate for taking such risk.

4.3.4.20. The source and/or origin of wealth is something else than the source and origin of the funds used in a transaction (compare the following with point 4.4.3 of these Guidelines, where the requirements for identifying the source and origin of funds used in a transaction are listed). Establishment of the source and/or origin of wealth means that the obliged entity identifies a bigger and more general picture of the customer's wealth, i.e. the source of all assets. This usually indicates how many funds the customer may have at all and where the customer received these funds from. In addition to requesting the relevant information from the customer, it may also be possible to collect such information from public databases and other public or non-public data, such as the land register, registers of other assets, declarations of economic interests, registers of companies, etc. However, the data of the source and/or origin of wealth must be verified on the basis of reliable and independent data, documents and information if the risk associated with the customer is particularly high. The obliged entity should not settle for the general answers of the customer or make unjustified assumptions (e.g. that employees with significant functions have bigger salaries and more assets etc.) and the obliged entity must be convinced that they know the source and/or origin of the customer's wealth. If the customer refuses to disclose data about the source and/or origin of their wealth or gives general answers or the data differ from the data that are publicly or non-publicly accessible, this may be a situation that points at a higher risk to which enhanced attention must be given, i.e. with regard to which enhanced measures must be taken.

Data retention

4.3.4.21. The obliged entity registers and retains information about all actions undertaken to identify a politically exposed person, i.e. the consideration about the determination or non-determination of the high-risk status. The obliged entity also retains all the data found in the course of these actions. The obliged entity does the above on the basis of point 5 of these Guidelines.

4.3.5. <u>Identification of the source and/or origin of wealth</u>

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

4.3.5.2. In the case of an occasional transaction outside a business relationship, the obliged entity collects information about the source and/or origin of the wealth instead of the purpose and nature of the business relationship (within the meaning of point 4.3.6 of these Guidelines) in the appropriate case. The obliged entity also takes other measures if necessary, which are stipulated under the identification of the purpose and nature of a business relationship within the meaning of point 4.3.6 of these Guidelines.

4.3.5.3. Within the meaning of these Guidelines, identification of the source and/or origin of wealth means the measures described in point 4.3.4.20 of these Guidelines.

4.3.6. Identification of the purpose and nature of a business relationship or occasional transaction

General principles

4.3.6.1. In the case of the establishment of a business relationship or an occasional transaction, the obliged entity must understand the purpose and nature of the business relationship or transaction. This is one, but a significant, part of the implementation of the Know-Your-Customer principle[126].

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

Purpose of measures taken in appropriate case

4.3.6.3. The additional measure specified in point 4.3.6.2 of these Guidelines means, among others, making queries in public sources[127] and additional information is ascertaining the permanent area of activity, payment practices, main transaction partners and, in the case of a legal entity, the experience of the customer or the person participating in an occasional transaction. The above is not an exhaustive list and, if necessary, the obliged entity takes additional measures to understand the purpose and nature of the business relationship, incl. primarily identifies the source and/or origin of wealth, where necessary, and performs on-site visits before the establishment of the business relationship[128], etc. In the case of certain services, the aforementioned circumstances can be partially or fully ascertained within the framework of the other obligations to be performed by the obliged entity (e.g. compliance with the principle of responsible lending, ascertainment of investment interests) or they are part of the service (e.g. time of loan repayments or realisation of an investment, etc.).

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

[126] See also point 4.1.4.2 of these Guidelines.
[127] Internet searches, use of Google Maps to find information about the place of business, etc.
[128] The purpose is to understand whether the information submitted by the customer corresponds to reality.

international sanctions or that the transactions of the customer are attempts to avoid an international sanction.

4.3.6.5. If the objective on one hand is to obtain a comprehensive understanding and overview of the customer (point 4.3.6.4 of these Guidelines), the objective is also to understand and ensure that such a wish of the customer complies with their actual activities, capability, capacity and needs. In such a manner, the identification of the purpose and nature cannot often be limited to mere collection of information, because this would not in reality give the obliged entity the kind of overview of the customer that enables the obliged entity to understand the customer, the customer's activity profile, the purpose of the transaction and the source and origin of the funds. As indicated below (area of activity, payment practices, main business partners and specifics requested in the course of experience), asking about one circumstance is not separate from asking other questions necessary for the identification of the purpose and nature of the business relationship. This means that the area of activity must correspond with the customer's payment practices and the extent and volume in which the customer performs transactions in the course of the business relationship, and the main business partners must be those with whom transactions will be concluded in this area of activity and with these transaction volumes, whilst the customer must also have the relevant experience for this, i.e. experience in the area of activity, to perform transactions with these business volumes, having the relevant (business) relationships.

4.3.6.6. In the appropriate case the obliged entity also ascertains whether the customer is a part of a larger group of companies, i.e. a group of related companies, and in such a case applies due diligence measures for the group of customers jointly as well as individually at the level of the individual group member. In respect of a customer group the task of the obliged entity, in addition to ordinary due diligence measures, is to ascertain the reason why obtaining the service via different group companies was chosen, what the role of each group company is, whether the group companies intend to conclude transactions with each other and what the legal and economic purpose of the transactions are (incl. that a fictitious intermediary has not been created for the purpose of transferring funds), whether the Internet banking solution will be logged in from the same IP addresses (who this person is and why one person manages all of the transactions). Also, it must be taken into account primarily upon the ascertainment of experience and payment practices that in a situation where the representative and/or the beneficial owners are the same, the experience of these persons must cover all of the areas of activity and the existence of (business) relationships with one or all of the main business partners of each group company and the payment practices must reflect the capability and experience of this one representative and/or beneficial owner (see also points 4.3.6.24 to 4.3.6.27 of these Guidelines).

4.3.6.7. The objective of identifying the purpose and nature of the business relationship or occasional transaction is, among others, to identify the circumstances referring to the risks specified in Annexes 1 and 2 of these Guidelines and to take relevant measures. Obliged entities must keep in mind that several characteristics that refer to risks together or separately may be a sign of the use of a shell company[129] or of other suspicious and unusual activity that does not refer to reasonable economic activities, in which case the obliged entities must also explain to Finantsinspektsioon, where necessary, why the obliged entity has established a business relationship that corresponds to such characteristics and why it is continued.

[129] In English – shell company. The FATF has defined the term 'shell company' in many of its guidelines as a company that does not have independent activities, notable assets, continuing business activities or employees, but it may also be a case of the activities of a shell company if, in addition to the aforementioned characteristics, a place of business is used that does not correspond to the conditions necessary for its activities, labour or other taxes are not paid, and there are large or rather large turnovers but no income seems to be earned from these.

4.3.6.8. As is the case with all other due diligence measures, the risk-based approach stipulated in point 4.2 of these Guidelines must be proceeded from when the purpose and nature of the business relationship are identified. The bigger the risk associated with the customer, the more measures the obliged entity must take to understand the customer and their risk profile and to understand whether the Know-Your-Customer principle has been followed and whether it is unambiguously understandable which service the customer wants to get and why, i.e. whether this wish corresponds to their actual activities, capacity and needs. Information may not be vague in such cases[130].

4.3.6.9. The additional measures and exceptions concerning life insurance undertakings, creditors and credit intermediaries and fund management companies have been specified in points 4.7.1, 4.7.2 and 4.7.3 of these Guidelines, respectively.

Area of activity

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

4.3.6.11. The accuracy of the area of activity defined by the customer must correspond to the risk profile of the customer and the business relationship and the customer's risk level. Thus, in the case of a risk that is higher than usual, this may not be economically unreasonably too broad[131] or economically unreasonably completely different from each other[132], which is why the area of activity allows the customer to basically deal with everything and does not allow the obliged entity to correctly monitor the business relationship.

4.3.6.12. Upon the identification of the area of activity, the obliged entity must also identify whether an authorisation for provision of a financial service is required for the service to be provided and whether the service is actually provided via the obliged entity to the customer's customers, i.e. to the ultimate beneficial owners to whom the obliged entity should apply due diligence measures (with the exceptions specified in point 4.8.3 of these Guidelines).

4.3.6.13. All in all, the identification of the area of activity must comply with the general principles of identification of the purpose and nature of a business relationship within the meaning of points 4.3.6.4 and 4.3.6.5 of these Guidelines and allow for these circumstances to be identified.

Payment practices

4.3.6.14. In the case payment practices, it is important to identify the manner in which financial services are consumed, incl. for example (i) the approximate number, volume, purpose and frequency

[130] This means that information, incl. information about transactions, may not often be vague, i.e. based on an abstract description. In the case of an abstract description, the obliged entity will not and cannot study the data in depth and ensure that they know the customer and have an adequate overview of them in order to monitor the customer's transactions against said information later, i.e. ensure that the transactions and acts performed within the scope of the business relationship primarily correspond to the information collected about the customer during the business relationship.

[131] For example, construction or construction materials may basically mean anything, as it is possible to build roads, planes, houses, ships, bridges, etc. Also, construction equipment may include small tools as well as big cranes, plant fittings, etc. Or wholesale, which may also cover buying and selling basically everything.

[132] For example, purchase and sale of food products on one hand and construction on the other, etc. (this is intentionally worded broadly and the principle that an area of activity may not be too broadly defined has not been considered, because the purpose is to describe different categories of areas of activity).

of transactions concluded per month and per year, the countries from which payments are received and to which payments are made, the expected duration of the business relationship, the extent and channels of cash use, payment channels (branch, Internet bank, card payments), etc.[133]; (ii) the frequency, size and time of repayments related to the loan taken within the scope of the business relationship to be established; (iii) in the case of investment products, the recommended securities, the approximate quantities in which they will be purchased and the frequency of purchases, the information related to their realisation, the quantity of assets to be invested, the expected duration of the business relationship (one-off activity or similar activities), etc. The obliged entity assesses the above circumstances in conjunction with the circumstances specified in Annexes 1 and 2 of these Guidelines.

4.3.6.15. The obliged entity must thereby identify whether, why and on which conditions the customer is capable of concluding such transactions at all[134] and how this corresponds to the customer's knowledge in other respects and the risk profile of the customer and the business relationship in general. The performance of this obligation often calls for the more general identification of the source and/or origin of the customer's wealth.

4.3.6.16. All in all, the identification of the payment practices must comply with the general principles of identification of the purpose and nature of a business relationship within the meaning of points 4.3.6.4 and 4.3.6.5 of these Guidelines and allow for these circumstances to be identified.

Main business partners

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

4.3.6.18. The main business partners means the persons who make the conclusion of incoming and outgoing transactions possible[135], i.e. the main business partners must be identified in two separate categories.

4.3.6.19. The obliged entity must in the appropriate case, but primarily in the case of a risk that is higher than usual, also ascertain how these main business partners are associated with the area of activity, i.e. whether the information that also confirms activities in said area of activity is publicly accessible. The obliged entity must also ascertain in the appropriate case why these main business partners agree or are prepared (incl. on which preconditions[136]) to conduct business with the customer, and this obligation primarily lies in the situation where the customer is a newly established company or a so-called shell company[137] that was previously established, but starts conducting business at the specific moment in time.

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

---

[133] In appropriate cases also, for example, whether the customer concludes transactions with goods of dual use, goods on which an embargo or export-import restrictions have been established, whether the goods are transported to sanctioned countries (even if the goods are unloaded in another country within the scope of this specific business relationship), whether prepayments are usually made for the goods or they are paid for upon receipt, etc.

[134] For example, requesting an annual report and comparing the data therein with the planned activities may also be relevant.

[135] For example, in the case of purchase and sale of goods, who the persons from whom goods are purchased are and to whom they are sold.

[136] For example, prepayments, etc. and the actual compliance with their preconditions.

[137] In English – shelf company.

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

4.3.6.22. As the business partners in question are main business partners, the obliged entity must make sure upon the establishment of the business relationship that transactions will really be concluded with these persons. The obliged entity will check this circumstance later in the course of the business relationship.

4.3.6.23. All in all, the identification of the main business partners must comply with the general principles of identification of the purpose and nature of a business relationship within the meaning of points 4.3.6.4 and 4.3.6.5 of these Guidelines and allow for these circumstances to be identified.

Experience of representative (or key persons) and the beneficial owner

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

4.3.6.25. Thus the obliged entity has to identify where the representative's and/or beneficial owner's capacity, capability, skills and knowledge (experience in general) comes from in order to operate in this area of activity, with these business volumes and with these main business partners.

4.3.6.26. The identification of experience is often not limited to just requesting CVs, but requires a substantive understanding and analysis of how the customer's previous knowledge fits into the customer's business activity[138]. Consequently, it has to be established whether the business relationship or transactions are in compliance with the customer's ordinary participation in commerce and whether the business relationship or transaction has a clear economic reason.

4.3.6.27. All in all, the identification of the experience must comply with the general principles of identification of the purpose and nature of a business relationship within the meaning of points 4.3.6.4 and 4.3.6.5 of these Guidelines and allow for these circumstances to be identified.

Data retention

4.3.6.28. The obliged entity registers and retains information about all acts undertaken to identify the purpose and nature of the business relationship and the occasional transaction. The obliged entity also retains all the data found in the course of these actions. The obliged entity does the above on the basis of point 5 of these Guidelines.

4.4. Due diligence measures during the business relationship

4.4.1. Updating data

[138] For example, everyone may have worked in a large company, but this does not give the capacity, capability, skills and knowledge to conduct business in the declared area of activity, with the declared business volumes and with the main business partners.

4.4.1.1. The obliged entity ensures that the documents, data or information collected in the course of the application of due diligence measures are updated regularly and in the case of trigger events[139], i.e. primarily the data concerning the person, their representative (incl. the right of representation) and beneficial owner as well as the purpose and nature of the business relationship.

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

4.4.1.3. The obliged entity will thereby decide the manner in which the data are updated, assessing the risk associated with the customer and the business relationship and the extent to which data can be updated by indirect measures without having to intervene in the usual functioning of the customer relationship[140].

4.4.2. Ongoing monitoring of business relationship

General principles

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

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

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

4.4.2.4. In such a manner, the obliged entity constantly assesses whether the purpose and nature of each single transaction correspond to what was already ascertained in the course of the

[139] In English – trigger event.

[140] For example, updating data by indirect methods may be appropriate in the case of customers who are natural persons, whose risk is lower than usual or average, who use ordinary settlement services and/or repay a loan in the ordinary manner, incl. the payment discipline of the person, the ordinary nature of the transactions carried out in the account, etc., which give no reason to believe that the data specified in point 4.3 of these Guidelines have changed (the person still receives their salary from the same place or is paid a pension, the person still visits grocery stores in the same city or pays the same entity for utilities, etc.).

application of due diligence measures upon the establishment of the business relationship, i.e. the information previously known about the customer. The obliged entity must thereby select the suitable scope of implementation of due diligence and, based on this, collect sufficient data and documents. The objective is to obtain an adequate overview of the customer or the person taking part in the transaction, incl. an overview of the customer and the customer's profile, and the reasons why the specific transaction is concluded and within the scope of which economic or legal relationships the customer concludes transactions, in order to assess, if necessary, whether it corresponds to the information already known.

4.4.2.5. As is the case with all other due diligence measures, the risk-based approach stipulated in point 4.2 of these Guidelines must be followed here as well. The higher the risk/threat associated with the customer, the more the obliged entity must take measures to understand the customer and their risk profile and the single transaction carried out within the scope of the business relationship and be sure that it corresponds to the information previously known about the customer. Information may not be vague in such cases[141].

4.4.2.6. In a situation where the data collected in the course of the application of due diligence measures, i.e. in this case during the ongoing monitoring of the business relationship, are not sufficient or they are contradicting or their authenticity can be doubted in any other manner, the obliged entity cannot obtain an adequate overview or the reassurance that the customer's transactions correspond to the previously identified purpose of the transaction and the customer profile in general. In this case, the obliged entity cannot correctly identify the purpose for which the customer wants to conclude a single transaction. In said case, the obliged entity has not applied due diligence measures sufficiently and has failed to monitor the business relationship correctly. The consequence is that the obliged entity must apply due diligence measures again as required by points 4.1.7.3 and 4.1.7.4 of these Guidelines. This is the same as if the obliged entity had not adequately applied due diligence measures from the beginning.

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

4.4.2.8. The additional measures and exceptions concerning life insurance undertakings, creditors and credit intermediaries and fund management companies have been specified in points 4.7.1, 4.7.2 and 4.7.3 of these Guidelines, respectively.

4.4.2.9. Transaction monitoring measures are divided into two categories: measures that can be used to monitor (screen[142]) transactions in real time on the basis of the parameters or characteristics developed according to the previous work experience of the obliged entity (IT measures) and measures that can be used to analyse (monitor[143]) transactions later.

4.4.2.10. The objective of monitoring the business relationship is, among others, to identify the circumstances referring to the risks specified in Annexes 1 and 2 of these Guidelines and the implementation of relevant measures. Obliged entities must keep in mind that several

[141] This means that information, incl. information about transactions, may not often be vague, i.e. based on an abstract description. In the case of an abstract description, the obliged entity will not and cannot study the data in depth and ensure that the customer's activities correspond to the information collected about them, because in this manner the obliged entity does not obtain the kind of overview of the customer that would allow the obliged entity to understand the customer, the customer's activity profile, purpose of the transaction and the source and origin of the funds.

[142] In English – screening.

[143] In English – monitoring.

characteristics that refer to risks together or separately may be a sign of the use of a shell company[144] or of other suspicious and unusual activity that does not refer to reasonable economic activities, in which case the obliged entities must also explain to Finantsinspektsioon, where necessary, why the obliged entity has established a business relationship that corresponds to such characteristics and why it is continued.

Screening

4.4.2.11. The monitoring of complicated, high-value and unusual transactions and transaction patterns that have no reasonable or obvious economic or legitimate purpose or that are uncharacteristic of the specific features of the business in question[145] forms a significant part of the due diligence measures implemented by the obliged entity and makes it possible to identify circumstances in the economic activities of customers that may refer to money laundering and terrorist financing. The monitoring of business relationships for the aforementioned purposes also has a role in the identification of subjects of international sanctions or transactions restricted with sanctions and politically exposed persons.

4.4.2.12. According to the monitoring of transactions in real time, customer service employees and other employees of the bank (see point 3.5 of these Guidelines about roles) monitor the customer's behaviour and transactions upon the performance of their duties in order to identify (i) suspicious and unusual transactions and transaction patterns, (ii) transactions that exceed the established thresholds, or (iii) politically exposed persons and circumstances related to international sanctions.

4.4.2.13. The obliged entity can do the following to monitor business relationships and transactions in real time as described:

i. build an IT solution, i.e. automatic IT systems that select real time transactions on the basis of the parameters given; and/or

ii. assign an employee of the obliged entity the obligation to review transactions manually; or

iii. use a combination of the above two measures.

4.4.2.14. The measures taken to monitor a business relationship in real time must be risk-based, i.e. comply with the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and risks arising from activities of the obliged entity. This means that the bigger the customer base of the obliged entity (the obliged entity cannot monitor transactions manually) and the higher the risk that criminal proceeds may be legalised (i.e. laundered)[146] or terrorism may be financed[147] via the services provided by the obliged entity, the more or the more extensive measures the obliged entity must take from among the measures specified in point 4.4.2.13 of these Guidelines.

4.4.2.15. If obliged entities use automatic systems to identify suspicious and unusual transactions carried out within the scope of specific business relationships, they should ensure that these systems

[144] The FATF has defined the term 'shell company' in many of its guidelines as a company that does not have independent activities, notable assets, continuing business activities or employees, but it may also be a case of the activities of a shell company if, in addition to the aforementioned characteristics, a place of business is used that does not correspond to the conditions necessary for its activities, labour or other taxes are not paid, and there are large or rather large turnovers but no income seems to be earned from these.

[145] These transactions and transaction patterns have hereinafter been referred to as *suspicious and unusual transactions* within the meaning of this sub-chapter on screening and monitoring.

[146] See also Annex 1 to these Guidelines.

[147] See also Annex 2 to these Guidelines.

are expedient, i.e. they should be consistent with the size of the obliged entity and the nature, scope and level of complexity of the activities and services provided, incl. the risk appetite and risks arising from activities of the obliged entity.

4.4.2.16. Considering that the purpose of monitoring business relationships in real time is to identify (i) suspicious and unusual transactions and transaction patterns, (ii) transactions that exceed the established thresholds, or (iii) politically exposed persons and circumstances related to international sanctions, the parameters / case scenarios of the automatic IT system must:

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

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

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

iv. in order to identify a subject of international sanctions, cover the capability to verify the compliance of data in respect of the customer, their representative and the beneficial owner[148];

v. in order to identify politically exposed persons, cover the capability to verify the compliance of data in respect of the customer, their representative and the beneficial owner[149];

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

vii. ensure that the obliged entity can identify concealed or obvious (business) ties between different customers (e.g. belonging to the same group) of which the obliged entity was previously not aware (see also points 4.4.3.8 and 8.4 of these Guidelines).

4.4.2.17. Upon the selection of an automatic IT system, the obliged entity must ensure that such monitoring takes place at least once a week, excl. sub-points 1-3 of point 4.4.2.16 of these Guidelines, which has to take place in real time, also excl. sub-point 4, which must also take

[148] The obliged entity must thereby consider the extent to which the data collected during general due diligence measures (incl. the data collected in the course of monitoring) are relied on or to which all owners (i.e. persons whose shareholding is less than 25%) should also be registered in databases in addition to the beneficial owner, keeping in mind that pursuant to the FATF requirements, a person who has control in any other manner must also be identified in relation to the sanctions, i.e. persons whose shareholding is less than 25% must also be included.

[149] The obliged entity must thereby consider the extent to which the data collected during general due diligence measures (incl. the data collected in the course of monitoring) are relied on or to which all owners (i.e. persons whose shareholding is less than 25%) should also be registered in databases in addition to the beneficial owner, keeping in mind that pursuant to the FATF requirements, a person who has control in any other manner must also be identified in relation to the sanctions, i.e. persons whose shareholding is less than 25% must also be included.

place in real time if the obliged entity does not take measures every time when changes are made in international financial sanctions.

4.4.2.18. If the obliged entity does not select an appropriate IT system, their manual monitoring systems must cover the principles stipulated in point 4.4.2.16 of these Guidelines.

4.4.2.19. In any case, the obliged entity is ready to justify to Finantsinspektsioon why the obliged entity selected the respective solution for monitoring (screening) business relationships and, in the appropriate case, why the circumstances and risks specified in point 4.4.2.14 of these Guidelines are not present. The obliged entity is also ready to justify why the specific parameters / case scenarios have been selected.

Monitoring

4.4.2.20. Transactions that have been separated from the mass of transactions later on the basis of certain parameters are analysed for monitoring.

4.4.2.21. According to transaction monitoring, customer service employees and other employees of the bank (see point 3.5 of these Guidelines for roles) observe the customer's behaviour and transactions upon the performance of their duties in order to identify transactions and circumstances that could not be identified in real time (they could not be intervened in, such as transactions made via ATMs) or that, due to the nature of the transaction, did not appear in the parameters of monitoring transactions in real time in the case of the IT solution or in acts in the case of manual monitoring (e.g. larger transactions by amounts, currencies or customer types).

4.4.2.22. Below are examples of some typical parameters[150] on the basis of which transactions can be selected for monitoring and which may not appear under the parameters of real time monitoring:

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

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

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

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

v. unexpected increase in the turnover of VOSTRO accounts in correspondent relationships[151];

vi. transactions of a certain customer (type).

Transactions indicating higher risk

4.4.2.23. Pursuant to point 4.2.6.4 of these Guidelines, the obliged entity must pay enhanced attention or apply enhanced due diligence measures to transactions and transaction patterns that are

[150] The obliged entity may also use other principles of transaction monitoring.
[151] Incl. in those that are not high-risk correspondent relationships.

complicated, high-value and unusual and that have no reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

4.4.2.24. In addition to the application of enhanced due diligence measures, the background of each single transaction specified in point 4.4.2.23 of these Guidelines must be investigated to the extent that is reasonably necessary, incl. the details of the transaction must be specified and any circumstances that have emerged must be analysed in order to identify the most typical features of the most frequent transactions. These data must be retained. The main circumstances to which attention must be given in analysing such transactions are as follows:

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

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

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

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

v. whether the obligation to report to the Financial Intelligence Unit must be performed within the meaning of point 7 of these Guidelines.

Customer visits

4.4.2.25. The monitoring of business relationships cannot in certain cases be comprehensively applied primarily in the event of customers whose risk is higher than usual if the obliged entity (i.e. primarily a credit institution) does not perform on-site visits to the customer to check whether the customer's explanations of their capability and capacity are true. In this manner, an on-site visit to the customer is a part of the obligation to monitor business relationships, especially in the situations where the obliged entity does not have a branch or other solution at the location of the customer's activities that would allow it to know what is going on in the target country and thereby know whether the customer is capable of performing such transactions in such volumes.

Data retention

4.4.2.26. The obliged entity registers and retains information about all acts carried out to ongoing monitor the business relationship, i.e. check whether the transactions carried out by the customer correspond to what the obliged entity knew about the customer before. This also covers the investigation of transactions that have been described in point 4.4.2.23 of these Guidelines. The obliged entity also retains all the data found in the course of these actions. The obliged entity does the above on the basis of point 5 of these Guidelines.

4.4.3. Identification of the source and origin of funds used in a transaction

General principles

4.4.3.1. In the course of the business relationship, the obliged entity identifies the source and origin of the funds used in a transaction if necessary.

4.4.3.2. Asking about the source and origin of the funds used in the transaction is basically equivalent to the monitoring of the business relationship within the meaning of point 4.4.2 of these Guidelines and the objective provided therein, with the difference being that whilst the monitoring of the business relationship covers the entire business relationship of the customer and its lifecycle, the source and origin of the funds used in a transaction are only related to incoming transactions. However, the goal is still the same – to obtain an adequate overview of the customer and find out whether this corresponds to the information previously known about the customer. This is why all of the explanations under the general principles of point 4.4.2 of these Guidelines apply to the source and origin of the funds used in the transaction.

4.4.3.3. The explanations under the general principles of point 4.4.2 of these Guidelines, which explain the scope of the application of due diligence measures, i.e. which characteristics the collected information must correspond to (incl. the opposite, i.e. which characteristics it may not correspond to), also apply.

The need to identify the source and origin of funds used in a transaction

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

i. proportionally to the size of the funds;

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

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

iv. if the obliged entity suspects that the transactions indicate criminal activities, money laundering or terrorist financing or that the relation of transactions to money laundering or terrorist financing is probable, incl. complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

Source and origin of funds

4.4.3.5. The legislator has intentionally differentiated between the source and origin of the funds used in a transaction. The source is thereby the reason, explanation and basis (legal relationship and its content) why the funds were transferred. The origin is broader and includes the activity with

which the funds were earned or received and is closer to the identification of the source and/or origin of wealth (see also point 4.3.5 of these Guidelines).

4.4.3.6. The need to identify the source of funds with relevant data increases if the bases specified in point 4.4.3.4 of these Guidelines are present. Identification of the origin of funds depends on the relevant situation, considering the risk-based approach and the extent to which the obliged entity must identify the origin of the source of the funds in order to obtain reassurance.

4.4.3.7. Asking about the source and origin of the funds used in a transaction does not mean the knowing or understanding which credit institution and which person the payment was received from and what its details were. The obliged entity cannot leave the source and origin of the funds unidentified either, as the funds come from another credit or payment institution that also implements equivalent due diligence measures.

4.4.3.8. If the obliged entity suspects that the information related to the payer is not correct in the case of an incoming payment, i.e. this is actually a payment in a longer chain (see also point 8.4 of these Guidelines), the identification of the source and origin of the funds used in the transaction requires performance of the obligation in respect of the first link or chain of the transaction, i.e. the initial source and origin of the assets (the person from whom the funds initially started moving from in this chain).

Data retention

4.4.3.9. The obliged entity registers and retains information about all acts undertaken to identify the source and origin of the funds used in the transaction. The obliged entity also retains all the data found in the course of these actions. The obliged entity does the above on the basis of point 5 of these Guidelines.

4.5. Simplified due diligence measures

4.5.3. The obliged entity may apply simplified due diligence measures if they have identified according to point 4.2 of these Guidelines that the risk of money laundering or terrorist financing in the case of the customer and their activities is lower than usual.

4.5.4. Simplified due diligence measures can be applied to the customer upon the establishment of a business relationship or to the transaction carried out by the customer during the business relationship or in the case of an occasional transaction.

4.5.5. Irrespective of the customer being assigned a risk level that is lower than usual, simplified due diligence measures may only be applied to the transactions of the customer if at least the following conditions have been met:

4.5.5.1. a long-term contract has been entered into with the customer in written or electronic format or in a format that can be reproduced in writing;

4.5.5.2. the obliged entity receives payments within the scope of the business relationship only via an account located in a credit institution entered in the Commercial Register in Estonia or in a branch of a foreign credit institution or in a credit institution that has been established or whose place of business is in a contracting state of the European Economic Area or in a state where requirements equal to those established in the relevant directives of the European Parliament and of the Council[152] are implemented;

[152] See footnote 65 for the relevant directive of the European Parliament and of the Council.

4.5.5.3. the total value of the incoming or outgoing payments of transactions made in the business relationship does not exceed 15,000 euros per year.

4.5.6. The obliged entity considers the provisions of the Guidelines on Risk Factors[153] when deciding on the application of simplified due diligence measures to the customer or their transaction, whilst the simplified due diligence measures

4.5.6.1. upon establishment of a business relationship may, among others, be the following:

i. verifying the identity of the customer or their representative on the basis of information obtained from a reliable and independent source at the time of establishment of the business relationship if this is necessary in order to not disturb the ordinary course of business activities;

ii. assuming the nature and purpose of the business relationship, because the product has been created for one specific purpose only, e.g. for a company's pension scheme or the gift voucher of a shopping centre;

iii. obtaining information from the customer when the beneficial owner is checked, not from an independent source (this is not permitted when the identity of the customer is verified).

4.5.6.2. in the course of the ongoing monitoring of the business relationship may, among others, be the following:

i. adjustment of the frequency of updating and review of the due diligence measures implemented in respect of a customer in a business relationship, e.g. by only doing so if a certain trigger event[154] occurs, e.g. the customer starts using the funds in a term deposit, sells an investment, etc. (however, this may not lead to avoidance of the obligation to update or monitor data);

ii. adjustment of the frequency and intensity of transaction monitoring, e.g. by only monitoring transactions that have exceeded a certain threshold. If the company decides to do this, it must ensure that the threshold has been set at a reasonable level and systems have been established for the identification of related transactions that would exceed this threshold in total.

4.5.7. Irrespective of the application of simplified due diligence measures, the obliged entity must ensure adequate monitoring of the business relationship to be able to identify, among others, suspicious transactions (see also point 4.4.2 of these Guidelines) and make it possible to report to the Financial Intelligence Unit on suspicious transactions (see also point 7 of these Guidelines).

4.5.8. The information collected during the application of simplified due diligence measures to a customer must give the company the reassurance that its assessment that the risk associated with the customer or the business relationship is lower than usual is justified.

4.5.9. Upon the application of any due diligence measure, the obliged entity takes into account the money laundering and terrorist financing risks and methods specific to Estonia given in Annexes 1 and 2 to these Guidelines.

4.5.10. The obliged entity documents and, upon the demand of the supervisory authority, demonstrates why, in respect of what and which simplified due diligence measures the obliged entity has applied

[153] Guidelines on Risk Factors (footnote 64).
[154] In English – trigger event.

to the customer upon the establishment of the business relationship or in respect of transactions during the business relationship.

4.6. Enhanced due diligence measures

4.6.3. The obliged entity must apply enhanced due diligence measures if they have identified according to point 4.2 of these Guidelines that the risk of money laundering or terrorist financing in the case of the customer and their activities is higher than usual. Enhanced due diligence measures are applied in order to appropriately manage and mitigate the risk of money laundering and terrorist financing that is higher than usual.

4.6.4. An enhanced due diligence measure means that the obliged entity applies something in addition to the mandatory main due diligence measures.

4.6.5. Enhanced due diligence measures can be applied to the customer upon the establishment of a business relationship or to the transaction carried out by the customer during the business relationship or in the case of an occasional transaction.

4.6.6. The obliged entity considers the provisions of the Guidelines on Risk Factors[155] when deciding on the application of enhanced due diligence measures to the customer or their transaction, whilst enhanced due diligence measures always mean the reassessment of the customer's risk profile six months after the establishment of the business relationship. Enhanced due diligence measures may, among others, also be

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

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

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

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

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

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

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

ii. gathering additional information and documents regarding the actual execution of transactions made in the business relationship in order to rule out the ostensibility of the transactions (e.g. the existence of customs documents, goods insurance contracts, confirmations of payment of customs duties, special equipment (refrigeration equipment), etc.).

4.6.7. Upon the selection of enhanced due diligence measures, the obliged entity considers:

[155] Guidelines on Risk Factors (footnote 64).

4.6.7.1. among others, the money laundering and terrorist financing risks and methods specific to Estonia given in Annexes 1 and 2 to these Guidelines;

4.6.7.2. that the due diligence measure mitigates the identified higher-than-usual risk of money laundering and terrorist financing, is effective and proportionate in respect of this risk and takes it into account.

4.6.8. In addition to the ordinary enhanced due diligence measures, the measures specified in points 4.9 and 4.10 of these Guidelines must be applied in the case of a correspondent relationship with a respondent institution originating from a high-risk or third country and high-risk third parties.

4.6.9. Upon the application of any due diligence measure, the obliged entity takes into account the money laundering and terrorist financing risks and methods specific to Estonia given in Annexes 1 and 2 to these Guidelines.

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

4.7. Special cases of due diligence measures

4.7.1. Due diligence measures applied to life insurance undertakings

4.7.1.1. In the case of life insurance products, the obliged entity applies the due diligence measures described in these Guidelines with the differences specified below.

4.7.1.2. The name of the person determined as the beneficiary must be identified immediately after the determination of the person or after learning of the person.

4.7.1.3. Where the beneficiary is not determined by name, but based on certain characteristics[156] or in another manner, sufficient data must be gathered on the range of persons determined in such a manner so that it is proven that the identity of the beneficiary can be established at the time of executing a payment.

4.7.1.4. However, the identity of beneficiaries is verified at the time of executing a payment. Points 4.3.1 and 4.3.2 of these Guidelines will be taken into account upon the verification of identity (the latter point will apply if a legal entity can be determined as the beneficiary).

4.7.1.5. In a situation where a high-risk politically exposed person is determined as the beneficiary, the entire business relationship must be checked in detail before the payment is made and the senior management[157] of the obliged entity must be informed about this so it can make an informed decision about the associated risks and, if necessary, decide on the implementation of an additional measure, i.e. the so-called enhanced due diligence measures, by informing the Financial Intelligence Unit, etc. For this purpose, the life insurance undertaking ascertains according to point 4.3.4 of these Guidelines whether the beneficiary of the life insurance contract or their beneficial owner is a high-risk politically exposed person, a family member or a close associate of a politically exposed person.

4.7.1.6. If the policyholder transfers their rights and obligations arising from the life insurance contract to a third party by agreement with the obliged entity, the obliged entity must identify the

[156] In English – class of beneficiaries.

[157] Senior management within the meaning of these Guidelines has been defined in point 4.3.4.19 of these Guidelines.

person who takes over the contract at the time the contract is transferred and apply all due diligence measures to them. In such a case, the obliged entity must, in addition to the obligation set forth in point 4.7.1.5 of these Guidelines, identify whether the person who takes over the contract or their beneficial owner is a high-risk politically exposed person, their family member or close associate in addition to the beneficiary. The requirements stipulated in point 4.7.1.5 of these Guidelines must be implemented if such circumstances are ascertained in order to check the business relationship and inform the senior management[158] about the identification (see also point 4.3.4 of these Guidelines).

4.7.1.7. In the case of life insurance products the obliged entity must, considering the customer's risk profile and associated risks and the risk assessment of the obliged entity, in the relevant case identify *(i)* the connection between the policyholder and the insured person and the justification and understandability of such a connection, *(ii)* the connection between the policyholder and the beneficiary and the justification and understandability of such a connection and/or *(iii)* the connection between the insured person and the beneficiary and the justification and understandability of such a connection. The objective is to identify complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

4.7.1.8. In a situation where an insurance intermediary operates between the policyholder and the insurer, the person who applies the due diligence measures depends on the specific business model and the conditions determined by the parties in the contract. The possibility to rely on data collected by another party stipulated in point 4.8.2 of these Guidelines applies in this case. In any case, the customer, i.e. the policyholder, has a business relationship with the insurance intermediary as well as the insurer. Someone in said chain, i.e. the insurance intermediary or the insurer, must apply the due diligence measures subject to application upon the establishment of a business relationship and in the course of monitoring. If the insurance intermediary or the insurer does not apply due diligence measures in this chain, they must make sure and guarantee that the other obliged entity (i.e. the insurer in the case of the insurance intermediary and vice versa) implements them, entering into the relevant agreement that stipulates the obligations of the parties, if necessary. The above depends on the manner in which the insurance product is offered to the customer and how the customer performs their obligations (i.e. primarily the obligation to make payments) arising from the insurance contract. If another person is relied on, all the conditions, incl. at the level of contracts, of relying on another person must be complied with (see point 4.8.2 of these Guidelines).

4.7.2. Due diligence measures applied to creditors and credit intermediaries

4.7.2.1. In the case of credit intermediaries, the application of due diligence measures upon the establishment of a business relationship calls for the application of measures to the person who gives credit and to the person who borrows.

4.7.2.2. If the borrower transfers their rights and obligations arising from the loan agreement to a third party by agreement with the obliged entity, the obliged entity must identify the person who takes over the contract at the time the contract is transferred and apply all due diligence measures to them.

4.7.2.3. In the case of credit products the obliged entity must, considering the customer's risk profile and the associated risks as well as the risk assessment of the obliged entity, ascertain the connection between the borrower and the person who pays back the credit in the relevant case. The objective is to identify complicated, high-value and unusual transactions and

[158] Senior management within the meaning of these Guidelines has been defined in point 4.3.4.19 of these Guidelines.

transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

4.7.2.4. In a situation where a credit intermediary operates between the borrower and the creditor that holds an authorisation[159], the person who applies the due diligence measures depends on the specific business model and the conditions determined by the parties in the contract. The possibility to rely on data collected by another party stipulated in point 4.8.2 of these Guidelines applies in this case. In any case, the customer, i.e. the borrower, has a business relationship with the credit intermediary as well as the creditor. Someone in said chain, i.e. the credit intermediary or the creditor, must apply the due diligence measures subject to application upon the establishment of a business relationship and in the course of monitoring. If the credit intermediary or the creditor does not apply due diligence measures in this chain, they must make sure and guarantee that the other obliged entity (i.e. the creditor in the case of the credit intermediary and vice versa) implements them, entering into the relevant agreement that stipulates the obligations of the parties, if necessary. The above depends on the manner in which the credit is offered to the customer and how the customer performs their obligations (i.e. primarily the obligation to make payments) arising from the loan agreement. If another person is relied on, all the conditions, incl. at the level of contracts, of relying on another person must be complied with (see point 4.8.2 of these Guidelines).

4.7.3. Due diligence measures applied to fund management companies

4.7.3.1. In the case of transactions with fund units (and other instruments indicating a holding in a fund), the obliged entity applies the due diligence measures described in these Guidelines with the differences specified below.

4.7.3.2. In the case of transactions with fund units the obliged entity must, considering the customer's risk profile and associated risks and the risk assessment of the obliged entity, in the relevant case identify *(i)* the connection between the person who gave the purchase order of the fund unit and the person who paid for the unit and the justification and understandability of such a connection, and *(ii)* the connection between the person who gave the sale order of the fund unit and the recipient of funds received from the sale of the fund unit and the justification and understandability of such a connection. The objective is to identify complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.

4.8. Due diligence measures applied by another person

4.8.1. Outsourcing

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

4.8.1.2. The obliged entity outsources an activity in a situation where another person implements the requirements arising from the MLTFPA and/or these Guidelines on behalf and for the account

[159] This point applies to situations where the creditor is a licensed creditor and the case is not that of peer-to-peer loan intermediation.

of the obliged entity. This obligation differs from relying on another person where the other person implements the requirements arising from the MLTFPA and/or these Guidelines for the performance of their obligations arising from law, after which the obliged entity uses them in the performance of their obligations and relies on these data.

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

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

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

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

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

4.8.1.4. The obliged entity may outsource the obligation to fully or partly apply the due diligence measures specified in points 4.3.1 to 4.3.6 of these Guidelines (i.e. the identification of the customer, beneficial owner, politically exposed person, the source and/or origin of wealth and the purpose and nature of the business relationship) only:

i. to another obliged entity;

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

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

4.8.1.5. The obligation to apply due diligence measures not specified in point 4.8.1.4 of these Guidelines cannot be outsourced. This restriction does not apply to outsourcing activities related to the identification and implementation of international sanctions.[160]

4.8.1.6. The obliged entity selects the other person specified in the previous point with due diligence to ensure the capacity of this person to comply with the requirements of the MLTFPA and these Guidelines and ensure the reliability and necessary qualification of this person. When outsourcing the activity (activities) of the obliged entity, the obliged entity must ensure that the

[160] Although, for example, the obligation to identify an international sanction is performed via the application of due diligence measures upon the establishment of the business relationship (e.g. requesting information about a person and identification of beneficial owners under a possible sanction through, among others, the identification of the purpose and nature of the business relationship) as well as during the monitoring of the business relationship (e.g. whether the transaction counterparty is a sanctioned person or whether the performance of a transaction subject to a sanction is the object of the transaction), this is not an application of due diligence measures in its essence, but compliance with the International Sanctions Act and the legislation directly related thereto.

other person has the required knowledge and skills, primarily for identifying suspicious and unusual situations, and that they are capable of complying with all of the money laundering and terrorist financing prevention requirements stipulated by legislation. In order to comply with the provisions of this point, the obliged entity must make sure that the managers of the other entity are informed about the relevant requirements and ensure training of employees about the prevention of money laundering and terrorist financing within the scope described in point 3.7 of these Guidelines.

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

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

ii. that the outsourcing of the activity does not impede the activities of the obliged entity or performance of the obligations provided for in the MLTFPA and these Guidelines;

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

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

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

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

vii. that the obliged entity has the unrestricted right to inspect compliance with the requirements provided for in the MLTFPA and these Guidelines;

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

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

4.8.1.8. The situation where the application of due diligence measures to the required extent is not sufficiently possible or has been made impossible must be avoided in the course of the provision of the service(s) by another person. It must be possible for the other person to apply the necessary due diligence measures in full, and it must also be possible for them to immediately inform the contact person of the obliged entity and refuse the transaction.

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

4.8.1.10. The obliged entity immediately informs Finantsinspektsioon about entry into the contract that serves as a basis for outsourcing their activity (activities).

4.8.1.11. All of the money laundering and terrorist financing prevention requirements stipulated by legislation extend to the other person in respect of the outsourced activity (activities) within the meaning of point 4.8.1 of these Guidelines. The obliged entity that has outsourced an activity is responsible for compliance with requirements and therefore also for any violations.

4.8.1.12. Upon outsourcing an activity, the obliged entity also proceeds from the general outsourcing guideline of Finantsinspektsioon[161].

4.8.2. Relying on a third party

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

4.8.2.2. The obliged entity may rely on the data and documents gathered by another person upon the partial or full application of the due diligence measures specified in points 4.3.1 to 4.3.4 of these Guidelines (i.e. the identification of the customer, beneficial owner and politically exposed person) if the obliged entity:

i. gathers from the third party at least information on who is the person establishing the business relationship or making the transaction, their representative and the beneficial owner, as well as what is the purpose and nature of the business relationship or transaction;

ii. has ensured that, where necessary, it is able to immediately obtain all the data and documents whereby it relied on data gathered by another person;

iii. has established that the other person who is relied on is required to comply and actually complies with requirements equal to those established in the relevant directives of the European Parliament and of the Council[162], including requirements for the application of due diligence measures, identification of politically exposed persons and data retention, and is under or is prepared to be under state supervision regarding compliance with the requirements.

4.8.2.3. The obliged entity takes adequate measures to ensure performance of the obligations stipulated in point 4.8.2.2 of these Guidelines, incl. enters into a contract for this purpose if necessary and applies other measures.

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

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

[161] At the moment of establishment of these Guidelines, the guideline is titled “Requirements for outsourcing by subjects of financial supervision”.
[162] See footnote 65 for the relevant directive of the European Parliament and of the Council.

4.8.3. Failure to apply due diligence measures to ultimate beneficial owners

4.8.3.1. If the obliged entity provides a service to another credit or financial institution within the scope of a correspondent relationship[163] or a similar service where the customers of the credit institution or financial institution receiving the service benefit from the service (hereinafter the *beneficial customer*), the obliged entity does not have to apply due diligence measures to the beneficial customer within the meaning of the MLTFPA and these Guidelines upon performance of the obligations stipulated in point 4.9.6[164] of these Guidelines.

4.8.3.2. In any case, the obliged entity is responsible for compliance with the requirements arising from the MLTFPA and these Guidelines.

4.8.3.3. It is prohibited for the obliged entity to exercise such a right if the credit or financial institution that is their customer has been established in a high-risk third country or if the requirements stipulated in point 4.9.6[165] of these Guidelines have not been complied with.

4.9. Relationships with other credit or financial institutions and shell institutions

4.9.1. The obliged entity as a correspondent institution must have rules of procedure and an organisational solution in the case of any correspondent relationship[166] in order to identify suspicious and unusual transactions of the respondent institution[167] and their customers as well as the code of conduct of the correspondent institution upon the identification of said transactions.

4.9.2. The obliged entity as a correspondent institution must ensure in the case of each correspondent relationship that the respondent institutions have a separate account for serving customers and for the executing transactions related to their own economic activities.

4.9.3. The obliged entity as a correspondent institution must have rules for the establishment and maintenance of any correspondent relationship.

4.9.4. The obliged entity as a respondent institution or correspondent institution is not permitted to establish or continue a correspondent relationship with a shell credit or financial institution[168] or credit institutions or financial institutions that are known to allow shell credit or financial institutions to use their services. The obliged entity also assesses correspondent relationships with obliged entities of high-risk third countries, makes changes in them if necessary or terminates these business relationships.

---

[163] A correspondent relationship is:
1) the consistent and long-term provision of financial services by a credit institution (correspondent bank) to another credit institution (respondent bank), incl. the provision of a bank account, payment account or other account service and other related services such as cash management, international funds transfers, cheque clearing, payable through accounts and foreign exchange services;
2) the relationships between and among credit institutions and financial institutions, incl. where similar services are provided by a correspondent bank to a respondent bank for the purpose of servicing its customers, and incl. relationships established for securities transactions or funds transfers.

[164] Excl. point 4.9.6.8 if the institution is not a respondent institution of a high-risk or a third country.

[165] Excl. the exception specified in footnote 164.

[166] See footnote 163 for the definition of a correspondent relationship.

[167] I.e. with a respondent institution outside the European Union.

[168] Shell bank means a credit institution or financial institution, or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions, which is incorporated in a jurisdiction or country in which it has no management or administration or physical presence for purposeful business activities and which is unaffiliated with a regulated credit or financial group.

4.9.5. The obliged entity as a correspondent institution in a correspondent relationship must have measures for identifying whether the respondent institution is or has changed into a high-risk[169] or third country respondent institution, in which case the obligations stipulated in point 4.9.6 of these Guidelines must be performed.

4.9.6. An obliged entity as a correspondent institution that wants to establish a cross-border correspondent relationship with a high-risk or third country respondent institution must regularly apply the following requirements in addition to the ordinary enhanced due diligence measures (see primarily the requirements stipulated in points 4.3, 4.4 and 4.6 of these Guidelines about enhanced due diligence measures):

4.9.6.1. collect enough information about the respondent institution to fully understand the nature of the activities of the respondent institution and make a decision about the reputation and risks[170] of the relevant institution on the basis of publicly accessible information and assess whether this complies with the risk appetite and other principles of the correspondent institution;

4.9.6.2. ascertain that the respondent institution is under financial supervision and collect adequate information about the quality of supervision, incl. find out whether proceedings have been initiated against the institution in relation to breaches of legislation concerning the prevention of money laundering and terrorist financing;

4.9.6.3. ascertain that the respondent institution has an appropriate organisational solution for the prevention of money laundering and terrorist financing (incl. for the implementation of international sanctions and forwarding of information related to payments) and that it is obliged to apply and actually applies measures equal to those established in the relevant directives of the European Parliament and of the Council[171], incl. the requirements to apply due diligence measures and retain data. For this purpose, the obliged entity takes adequate measures and, among others, assesses the control systems of money laundering and terrorist financing prevention implemented and the measures taken in respect of customers in the respondent institution and makes sure that all of these are appropriate and effective and correspond to the size of the respondent institution and the nature, scope and level of complexity of the activities and services provided, incl. the risks arising from activities. Such assessment may occur as an on-site or remote inspection;

4.9.6.4. be aware of the risk structure of the beneficial customers, incl. which products and services the respondent institution offers, in which jurisdictions (target markets) and via which sales channels they do so, and monitor that the associated risk corresponds to the risk appetite of the obliged entity;

4.9.6.5. in the case of payable through accounts[172] make sure that the respondent institution has verified the identity of the customers who have direct access to the accounts of the correspondent institution, applies due diligence measures to them at all times and, upon request is able to present the relevant due diligence measures applied to the customer;

4.9.6.6. have measures to periodically ascertain whether any changes have occurred in respect of the respondent institution where the circumstance described in points 4.9.6.1 to 4.9.6.5 of these

[169] In any case, a high-risk respondent institution is an institution that is granted the right to use payable through accounts (see also footnote 172).
[170] This may cover, among others, an opinion of the country of the place of business of the respondent institution, its executive managers and ownership structure, and associated risks, incl. whether the respondent institution is in public or private ownership and what the risk associated with this is, whether the managers are politically exposed persons, etc.
[171] See footnote 65 for the relevant directive of the European Parliament and of the Council.
[172] In English – payable through accounts.

Guidelines are concerned, incl. apply the business relationship monitoring measures specified in point 4.4 of these Guidelines and, if necessary, apply appropriate measures;

4.9.6.7. document or determine by a contract or any other mutual agreement the relevant obligations of both institutions in the correspondent relationship and the rights[173] and obligations upon the application of due diligence measures, data retention and the exchange and forwarding of information as well as the reporting to the respective Financial Intelligence Unit;

4.9.6.8. receive the prior consent of the senior management for the establishment of a correspondent relationship with the respondent institution or for continuing the relationship already existing by the moment of the establishment of these Guidelines if an equivalent approval is missing.

4.9.7. If the respondent institution of a high-risk or third country is a subsidiary, the correspondent institution must assess the circumstances specified in points 4.9.6.1 to 4.9.6.2 also in the case of the parent company.

4.9.8. If another credit or financial institution uses correspondent services via a high-risk or third-country respondent institution (incl. if the respondent institution is a parent company via whom the subsidiary also uses the services of the correspondent bank), the circumstances specified in points 4.9.6.1 to 4.9.6.6 of these Guidelines must also be assessed in respect of this other credit or financial institution or, as an alternative, it must be made sure that the respondent institution has applied all of these measures to its own respondent institutions.

4.9.9. The obliged entity as a correspondent institution must have rules and define which respondent institutions are high-risk ones. The relevant rules must take into account point 4.2 of these Guidelines and the Guidelines on Risk Factors[174] (especially Chapter 1) and the relevant risk factors specified in the documents mentioned therein.

4.10. Transactions with natural persons and legal entities operating in high-risk third countries, incl. FATF high-risk or non-cooperative countries

4.10.1. If the obliged entity has contact[175] with a high-risk third country via a transaction carried out in their economic activities or a customer, they must apply the following due diligence measures in addition to the ordinary due diligence measures:

4.10.1.1. gathering additional information about the customer and their beneficial owner;

4.10.1.2. gathering additional information about the planned substance of the business relationship;

4.10.1.3. gathering information about the source and/or origin of the funds and wealth of the customer and their beneficial owner;

4.10.1.4. gathering information about the underlying reasons of planned or executed transactions;

4.10.1.5. obtaining permission from the senior management to establish or continue a business relationship;

[173] Incl. the respondent institution's right to provide correspondent services to other respondent institutions within the scope of the correspondent relationship and the right to immediately obtain all data and documents in order to identify the person who ultimately benefits from the transaction.
[174] Guidelines on Risk Factors (footnote 64).
[175] Having contact may mean, among others, that the customer is originally from or their place of residence or location or the location of the recipient of the payment or the payment service provider of the addressee of the payment is in said country or territory.

4.10.1.6. improving the monitoring of a business relationship by increasing the number and frequency of the applied control measures and by choosing transaction indicators that are additionally verified.

4.10.2. In addition to the above the obliged entity will, if necessary, apply the enhanced due diligence measures to be applied on the basis of point 4.6 of these Guidelines.

4.10.3. The obliged entity constantly monitors whether the relevant authorities of their country of operations or the country of operations of their representation, branch or subsidiary or the FATF have established additional countermeasures in respect of high-risk third countries, incl. the FATF high-risk or non-cooperative countries. The obliged entity applies these countermeasures and ensures that these measures are effective and proportional to the risks taken.

5. Data retention

5.1. The obliged entity must register and retain:

5.1.1. information about the circumstances of refusal of the establishment of a business relationship or the completing an occasional transaction by the obliged entity on the basis of point 6.1.1 of these Guidelines;

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

5.1.3. the circumstances of refusal to establish a business relationship or to conclude a transaction, incl. an occasional transaction, on the initiative of a person participating in the transaction or the customer if the refusal is related to the application of due diligence measures by the obliged entity;

5.1.4. originals or copies of the documents that serve as a basis for the establishment of identity and verification of the submitted information. If a person has been identified digitally, i.e. without being in the same place with the person, the data of the document for digital identification, the information about the making of an electronic query in the database of identity documents and the sound and video recording of the identification and verification procedure as well as other data (logs, etc.), which prove the verification of the data obtained in the course of identification (incl. the existence of two separate sources), must be registered and retained according to the selected measure. Data must not be registered and retained to the extent in which the obliged entity is capable of reproducing the aforementioned data during the five-year time period for data retention. The obliged entity must be capable of showing at all times that they have verified the data obtained in the course of identification and indicate the reliable and independent source of the data as well as the origin of the two sources;

5.1.5. the documents that serve as a basis for the establishment of the business relationship but not specified in point 5.1.4 of these Guidelines, incl. the documents collected for compliance with the requirements set out in point 4.3 of these Guidelines;

5.1.6. the transaction date or period and a description of the substance of the transaction;

5.1.7. also the following data in relation to transactions:

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

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

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

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

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

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

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

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

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

5.1.8. data and documents collected in the course of monitoring the business relationship, incl. the documents collected for compliance with the requirements specified in point 4.4 of these Guidelines (covering all analyses related to understanding transactions and measures for identifying the background and objective of complicated, high-value and unusual transactions and transaction patterns that do not have any reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question);

5.1.9. all of the correspondence related to the performance of the obligations arising from these Guidelines and the MLTFPA;

5.1.10. the information that serves as a basis for the obligation to report to the Financial Intelligence Unit;

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

5.1.12. information about the circumstances of termination of the business relationship within the meaning of point 6.3.3 of these Guidelines because the application of due diligence measures is impossible.

5.2. The data arising from point 5.1 (excl. point 5.1.10) of these Guidelines must be retained for five years after the expiry of the business relationship or the completion of an occasional transaction. The data related to the performance of the reporting obligation arising from point 5.1.10 must be retained for five years after the performance of the reporting obligation.

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

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

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

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

6. Refusal to establish business relationships and carry out transactions and (extraordinary) termination of business relationships

6.1. Refusal to establish business relationships or carry out occasional transactions

6.1.1. The obliged entity is prohibited to establish a business relationship or allow to execute an occasional transaction if:

6.1.1.1. they suspect money laundering or terrorist financing or it is impossible for the obliged entity to apply the due diligence measures taken upon the establishment of business relationships, because the customer does not submit the relevant data or refuses to submit them or the submitted data give no grounds for reassurance that the collected data are adequate;

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

6.1.1.3. a person who does not have the authorisation to operate as a credit or financial institution, but whose main and permanent economic activities via the obliged entity are similar or correspond to the provision of financial services subject to authorisation, wants to establish a business relationship or conclude an occasional transaction;

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

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

6.1.2. The obligation arising from point 6.1.1 of these Guidelines must not be performed if the obliged entity has informed the Financial Intelligence Unit about the establishment of the business relationship, an occasional transaction or an attempt to conclude a transaction pursuant to the procedure stipulated in point 7 of these Guidelines and/or received a specific instruction from the Financial Intelligence Unit to continue establishing the specific business relationship or concluding the occasional transaction.

6.1.3. In respect of the circumstances of refusal to establish a business relationship or conclude an occasional transaction, the obliged entity performs the reporting obligation according to the requirements set out in point 7 of these Guidelines and registers and retains the data of the refusal to establish a business relationship or conclude an occasional transaction as well as of the performance of the reporting obligation according to the requirements set out in point 5 of these Guidelines.

6.1.4. In a situation where the obliged entity constantly refuses to establish a business relationship or conclude an occasional transaction on the basis of point 6.1.1 of these Guidelines or if the above is refused before the application of due diligence measures, the obliged entity must carry out periodical analyses to identify:

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

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

6.2. Refusal to conclude a transaction within the scope of a business relationship

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

6.2.2. If a business relationship has not been established, the obliged entity may not establish a business relationship in the case of non-application of due diligence measures (see point 6.1.1 of these Guidelines). If the business relationship has been established and the due diligence measures cannot be applied again because the customer does not submit the relevant data, the obliged entity is required to terminate the long-term contract serving as a basis for the business relationship extraordinarily and without notice (see point 6.3.3 of these Guidelines). In addition to the obligation of extraordinary termination of a business relationship, the obliged entity has the right to refuse to conclude a transaction in certain cases. Not exercising this right in a situation where due diligence measures have not been applied or the need to apply them again arises because money laundering is suspected (see point 4.1.7.4 of these Guidelines) or the submitted data are not true (see point 4.1.7.3 of these Guidelines)[176] is only permitted in highly exceptional cases. Not exercising the right specified in point 6.2.1 is primarily permitted in the situation where not concluding the transaction is impossible or may obstruct the efforts made to capture the persons benefiting from the transaction or the capture of the person who is possibly laundering money or financing terrorism. For this purpose, the obliged entity cooperates with the Financial Intelligence Unit and in appropriate cases, complies with the reporting obligation within the meaning of point 7 of these Guidelines.

[176] In a situation where it becomes evident that the data collected in the course of the application of due diligence measures are not sufficient or they are contradicting or their authenticity can be doubted in any other manner and there are suspicions of money laundering, the obliged entity cannot obtain an adequate overview and the reassurance that they know the customer and the customer's transactions correspond to the previously identified purpose of the transaction and the customer profile in general. Thus, the obliged entity must apply due diligence measures again. This is therefore the same as if the obliged entity had not applied due diligence measures adequately from the beginning, which is why refusing to establish a business relationship is mandatory.

6.2.3. If the data are insufficient or untrue or if there are suspicions of money laundering or terrorist financing, the obliged entity must apply due diligence measures for as long as they have collected sufficient data, they are convinced that the data are true or until the suspicions of money laundering or terrorist financing are eliminated. The requirement arising from point 6.2.2 of these Guidelines that transactions may only be concluded under exceptional circumstances applies at the same time.

6.2.4. If the obliged entity has still not managed to apply adequate due diligence measures in the course of the activity stipulated in point 6.2.3 of these Guidelines within reasonable time in order to exhaustively collect data, make sure that the data are true or eliminate suspicions of money laundering or terrorist financing, the obliged entity must terminate the business relationship extraordinarily according to the requirements set forth in point 6.3.3 of these Guidelines.

6.2.5. The right arising from point 6.2.1 of these Guidelines must not be exercised if the obliged entity has informed the Financial Intelligence Unit about the business relationship transaction or attempted transaction pursuant to the procedure stipulated in point 7 of these Guidelines and received a specific instruction from the Financial Intelligence Unit to continue with the business relationship or the transaction. The right may also not be exercised if the obliged entity has received an instruction from the Financial Intelligence Unit without the prior relevant report.

6.3. (Extraordinary) termination of business relationships

6.3.1. The obliged entity can terminate the business relationships ordinarily and extraordinarily. In the case stipulated in point 6.3.2 of these Guidelines, the extraordinary cancellation of a business relationship is to be decided by the obliged entity themselves and in the case stipulated in point 6.3.3, the business relationship must be cancelled extraordinarily without notice.

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

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

6.3.2.2. money laundering is suspected in the case of the person, excl. the situation stipulated in point 6.2.4 of these Guidelines.

6.3.3. The obliged entity is required to terminate the long-term contract that serves as a basis for the business relationship extraordinarily without notice if the business relationship has been established and the due diligence measures cannot be applied again, because the circumstance specified in point 6.2.4 of these Guidelines are present or because the customer does not submit the relevant data or refuses to submit them or the submitted data give no grounds for reassurance that the collected data are adequate.

6.3.4. In the event of an extraordinary termination of a business relationship within the meaning of points 6.3.2 and 6.3.3 of these Guidelines, the obliged entity will transfer the customer's assets within reasonable time, but preferably not later than within one month[177] after the extraordinary termination of the business relationship and as a whole to an account opened in a credit institution entered in the Commercial Register in Estonia or in a branch of a foreign credit institution or a credit institution which is registered or whose place of business is in a contracting state of the European Economic Area or in a country where requirements equal those established in the relevant directives of the European Parliament and of the Council[178] are applied. In exceptional cases, assets may be transferred to an account other than the customer's account or issued in cash by informing the

[177] The obliged entity takes reasonable steps to do this within one month or as soon as possible.
[178] See footnote 65 for the relevant directive of the European Parliament and of the Council.

Financial Intelligence Unit about this with all the relevant and sufficient information[179] at least seven (7) working days in advance and on the condition that the Financial Intelligence Unit does not give a different order. Irrespective of the recipient of the funds, the minimum information given in English in the payment details of the transfer of the customer's assets is that the transfer is related to the extraordinary termination of the customer relationship.

6.3.5. The right arising from point 6.3.2 of these Guidelines must not be exercised and the obligation arising from point 6.3.3 must not be performed if the obliged entity has informed the Financial Intelligence Unit about the establishment of the business relationship, the transaction or attempted transaction pursuant to the procedure stipulated in point 7 of these Guidelines and received a specific instruction from the Financial Intelligence Unit to continue with the business relationship or the transaction. The right may also not be exercised if the obliged entity has received instructions from the Financial Intelligence Unit without the prior relevant report.

6.3.6. In respect of the circumstances of mandatory extraordinary termination of a business relationship, the obliged entity performs the reporting obligation according to the requirements set out in point 7 of these Guidelines and registers and retains the data of the extraordinary termination of the business relationship and the performance of the reporting obligation according to the requirements set out in point 5 of these Guidelines.

6.3.7. In a situation where the obliged entity constantly terminates business relationships extraordinarily on the basis of point 6.3.3 of these Guidelines, the obliged entity must carry out periodical analyses to identify:

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

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

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

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

7. Obligation to report to the Financial Intelligence Unit

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

7.1.1. the characteristics indicate the use of criminal proceeds or the commission of crimes related to this (this is primarily a report on a suspicious and unusual transaction or activity, i.e. UTR[180] or UAR[181]);

[179] Incl. the reason for termination of the business relationship, statement of account(s), the name of the other person who receives the funds and the details of the payment.
[180] In English – Unusual Transaction Report.
[181] In English – Unusual Activity Report.

7.1.2. in the case of which they suspect or know or the characteristics of which indicate the commission of money laundering or related crimes (this is primarily a report on a transaction or activity whereby money laundering is suspected, i.e. STR[182] or SAR[183]);

7.1.3. in the case of which they suspect or know or the characteristics of which indicate the commission of terrorist financing or related crimes (this is primarily a report on a transaction or activity whereby terrorist financing is suspected, i.e. TFR[184]);

7.1.4. in the case of which an attempt of the activity or circumstances specified in points 7.1.1 to 7.1.3 of these Guidelines is present.

7.2. The Financial Intelligence Unit must be notified:

7.2.1. by the obliged entity also about the circumstances of refusal of establishment of a business relationship or completing an occasional transaction on the basis of point 6.1.1 of these Guidelines and about the extraordinary termination of a business relationship on the basis of point 6.3.3 of these Guidelines (primarily a suspicious and unusual transaction or activity report, i.e. UAR);

7.2.2. by the obliged entity, except a credit institution, also about each transaction that has become known whereby a pecuniary obligation of over 32,000 euros or an equal sum in another currency is performed in cash, regardless of whether the transaction is made in a single payment or in several linked payments over a period of up to one year (primarily an amount-based report, i.e. CTR[185]).

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

7.3. The reports specified in points 7.1 and 7.2 of these Guidelines must be made before the completion of the transaction if the obliged entity suspects or knows that money laundering or terrorist financing or related crimes are being committed (see also point 6.2.5 of these Guidelines) and if said circumstances are identified before the completion of the transaction. Considering the speed at which money laundering and terrorist financing crimes are committed, such performance of the obligation to report before the completion of the transaction may also be appropriate in other cases[186]. If the postponement of the transaction may cause considerable harm, it is not possible to omit the transaction or it may impede capture of the person who committed possible money laundering or terrorist financing, the transaction will be concluded and a report will be submitted the Financial Intelligence Unit thereafter. The obliged entity is in contact with the Financial Intelligence Unit in order to identify such circumstances.

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

[182] In English – Suspicious Transaction Report.
[183] In English – Suspicious Activity Report.
[184] In English – Terrorist Financing Report.
[185] In English – Cash Transaction Report.
[186] For example, in a situation where the obliged entity concludes a transaction with which cash is paid out to the customer or the person participating in the transaction, the paid out cash becomes “invisible” because it is practically impossible to monitor the further movement of the funds, so in an ordinary situation and particularly in a situation where cash is paid out to the customer or the person participating in a transaction, which may mean that the funds cannot be monitored further, the obliged subject is required to perform the reporting obligation before the conclusion of the transaction if possible.

one working day, which is why quick reporting helps trace black money more efficiently.

7.5. In addition to the situation specified in point 7.3 of these Guidelines, the obliged entity must also wait for the feedback of the Financial Intelligence Unit in other appropriate cases before refusing to establish a business relationship (see also point 6.1.2 of these Guidelines) or before the extraordinary termination of a business relationship (see also point 6.3.5 of these Guidelines).

7.6. In a situation where, in the case of a so-called amount-based report or a report arising from the establishment or extraordinary termination of a business relationship and in respect of the customer or the circumstances related to them, the obliged entity has identified the activity or circumstances specified in point 7.1 of these Guidelines, the reporting obligation must also be performed within the meaning of point 7.1 of these Guidelines, whereby this may also take place within the scope of the same report, but by making reference to different indicators.

7.7. If the basis for compliance with the reporting obligation of the obliged entity is not a suspicion of money laundering or terrorist financing, but a so-called suspicious or unusual transaction and there are many such suspicious and unusual transactions and several reports have been made on the basis of these or the reports are continuing (and the making of such reports has not been extraordinarily agreed with the Financial Intelligence Unit), the obliged entity must start suspecting money laundering or terrorist financing, after which other due diligence measures have to be applied in addition to the relevant report and the refusal to conclude a transaction must be decided (see also points 6.2.3 and 6.2.4 of these Guidelines).

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

8. Forwarding of information related to payer and payee

8.1. The possibility to monitor money transfers fully may be a particularly important and valuable way for the prevention, detection and investigation of money laundering and terrorist financing and for the application of adequate measures. In order to ensure that information is passed on in the entire payment chain, the appropriate procedure has been established in the European Union in the format of Regulation (EU) No 2015/847 of the European Parliament and of the Council, pursuant to which payment service providers must forward information about the payer and the payee in transfers of funds.

8.2. Payment institutions and credit institutions acknowledge the existence of Regulation (EU) No 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds and the requirements arising therefrom, and comply with them.

8.3. Payment institutions and credit institutions comply with the requirements as (i) the payer’s payment service provider, as (ii) the payee’s payment service provider and as (iii) intermediary payment service provider.

8.4. Sending the information of the payer and the payee requires sending information about the persons who actually benefit from the payment. This means that in a situation where a payment institution or credit institution identifies a chain of transactions where the actual purpose of the transfers is to transfer the funds from one person to another until they are transferred to the beneficial owner, i.e. the ultimate addressee, the information of the beneficial owners (i.e. the actual payers and payees) must move through the entire payment chain.

9. Obligation to apply due diligence measures again

9.1. If necessary, the obliged entity will apply due diligence measures to existing customers again if they see that due diligence measures have not been adequately applied to existing customers in order to comply with the requirements set out in these Guidelines.

9.2. When assessing the need to apply due diligence measures, the obliged entity also proceeds from the customer's significance and risk profile and the time that has passed from the previous application of due diligence measures or the scope of their application.

9.3. The obliged entity reviews business relationships in order to identify whether one or several of the risk characteristics specified in Annexes 1 and 2 are present in the activities of their customers. The obliged entity takes the relevant measures, where necessary, to mitigate said risks and is prepared, where necessary, to comply with points 4.3.6.7 and 4.4.2.10 of these Guidelines.

10. Implementation of the Guidelines

Finantsinspektsioon gives market participants a transition period of three months for the implementation of these Guidelines, which starts from the enforcement of these Guidelines.

Annex 1 – Money laundering risks and methods specific to Estonia

Money laundering is divided into three phases:

1. placement;
2. layering;
3. integration.

The financial system of Estonia may be taken advantage of in different phases of money laundering. This Annex is based on different threat assessments, typologies, data accessible to Finantsinspektsioon, statistics, observations made during on-site inspections and special information. This takes into account the services and products offered by financial institutions and their volumes, and the geographic location of Estonia.

The biggest threats to Estonia are related to the phase of layering, where the criminal proceeds have been received in another country and they are given orders for making transfers on bank account or payment accounts (point (i) of layering) or attempts are made to conceal their actual origin, incl. by the so-called mirror transactions (point (ii) of layering).

Below is a list of products, services and ways through which Estonian financial institutions may primarily (this is not an exhaustive list) be abused for the purposes of money laundering and to which financial institutions should therefore give special attention. This overview is limited only to the financial institutions under the supervision of Finantsinspektsioon (credit institutions, fund management companies, investment firms, life insurance undertakings, payment institutions, creditors and credit intermediaries) and the products and services primarily offered by these financial institutions have been taken into account.

Some of the indicators listed in this Annex may also occur alone or together in regular and legitimate transactions, which is why the provided non-exhaustive list must be taken as a list that helps to identify the risks associated with the prevention of money laundering and terrorism.

1. Placement

Based on various threat assessments, typologies, the data accessible to Finantsinspektsioon, statistics, the observations made during on-site inspections and special information and considering the risks specific to Estonia, this phase of money laundering may be the following in the case of Estonia:

(i) funds are placed in a bank account or payment account in cash (so-called payment service);
(ii) various insurance premiums are paid and loans taken on the basis of loan agreements are repaid in cash, payments for fund units or other investment services are paid in cash, etc.;
(iii) criminal proceeds received from fraud, embezzlement, tax crimes, etc. are in the bank account or payment account at the moment the crime is committed, after which their legalisation starts.

Although the Know-Your-Customer principles is always applied upon the provision of financial services, i.e. the financial institution must always be convinced that it knows the customer, knows why the customer wants to receive the relevant financial service and knows that the customer's activities and conduct corresponds to the information known to the financial institution, in order to manage the risk of money laundering, the financial institutions should pay particular attention to the following in appropriate cases:

1. in the case of cash deposits:

    a. *the capability of the customer to conclude such a transaction* – the risks may be that the person who concludes the transaction makes a cash deposit in an amount that does not correspond to their ordinary capacity or seems unusual and does not correspond to the agreements made between the parties or the information declared by the customer;

    b. *the origin of the funds* – the risks may be that the source and origin of the funds used in the transaction cannot be identified or the explanation given about them is suspicious or unusual;

c. *the manner in which the customer was found* – the risks may be that the customer was introduced to the obliged entity by a third party, in the case of whom there may be a conflict of interests between the customer and the obliged entity, because, in addition to the role of introducing, the third party also provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;

d. *the risk arising from the person of the customer with the appropriate differences, which are specified under the risk arising from the person of the customer in sub-point 1 of point 2 (layering);*

2. in the case the obligations related to a financial service are paid in cash:

a. *the person who performed an obligation in cash* – the risks may be that a third party, incl. a party that has no connections to the customer, performs the financial obligation related to the financial service on behalf of the customer;

b. *the capability of the customer to conclude such a transaction* – the risks may be that the person who concludes the transaction pays for the obligations in an amount that does not correspond to their ordinary capacity or does not correspond to the agreements made between the parties in an unusual manner;

c. *the wishes and actual intent and capability of the customer* – the risks may be that the wish of the person who concludes the transaction and who wants to receive a specific financial service does not correspond to the activity expected from them and may not correspond to their actual intent;

d. *the manner in which the customer was found* – the risks may be that the customer was introduced to the obliged entity by a third party, in the case of whom there may be a conflict of interests between the customer and the obliged entity, because, in addition to the role of introducing, the third party also provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;

e. *the origin of the funds* – the risks may be that the source and origin of the funds used in the transaction cannot be identified or the explanation given about them is suspicious or unusual;

f. *the possible extraordinary nature of a repayment* – the risks may be that the customer performs a transaction related to the financial service earlier than expected (e.g. repays a loan early in an unusual manner, etc.);

g. *the other risks arising from the person of the customer with the appropriate differences, which are specified under the risk arising from the person of the customer in sub-point 1 of point 2 (layering).*

2. Layering

Based on various threat assessments, typologies, the data accessible to Finantsinspektsioon, statistics, the observations made during on-site inspections and special information and considering the risks specific to Estonia, this phase of money laundering may be the following in the case of Estonia:

(i) funds are transferred from one bank account or payment account to another or bank account and payment accounts are used to pay for various goods and services or to grant or repay loans;
(ii) customers purchase securities (in one currency and/or jurisdiction) and immediately sell them without reasonable economic purpose (in another currency and/or in another jurisdiction) or transfer

securities to their securities portfolio (in one jurisdiction) and immediately sell them without reasonable economic purpose (in another jurisdiction) (the above is in certain cases also known as mirror transactions);

(iii) a loan that was taken is repaid immediately or early, an insurance contract is terminated after a short time or early, fund units are sold immediately or after a short time, purchased securities are sold immediately or after a short time after their acquisition;

(iv) a third party pays for various insurance premiums, a loan taken on the basis of a loan agreement, fund units or a financial obligation related to another investment service or the payments are made in an amount that does not correspond to the customer's usual capacity;

(v) the funds in a bank account or payment account are withdrawn in cash and currency is also exchanged in the course of this activity in certain cases.

Although the Know-Your-Customer principles is always applied upon the provision of financial services, i.e. the financial institution must always be convinced that it knows the customer, knows why the customer wants to receive the relevant financial service and knows that the customer's activities and conduct corresponds to the information known to the financial institution, in order to manage the risk of money laundering, the financial institutions should pay particular attention to the following in appropriate cases:

1. in the case of payment services (transfer of funds)[187]:

    a. *the risk arising from the person of the customer* – the risks may be that (if one or several characteristics are present, depending on the situation):

        i. the person is a politically exposed person;

        ii. the person has or seems to have a connection to countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. areas of conflict, or countries that have other important connections with the aforementioned countries;

        iii. the person has no connection with Estonia, but they still want to receive the service in Estonia;

        iv. the person was established or originally from one country (e.g. address of the place of business), their beneficial owner is originally from another country (e.g. address of the place of residence), the current account has been opened in a third country and transactions are concluded with persons not associated with these countries (said conditions do not have to be present at the same time);

        v. the person carries out large transactions, whilst the representative and beneficial owner of the customer is the same person, incl. this person logs in to Internet bank solutions to conclude transactions themselves, and additional circumstances that are present may be that the incoming and outgoing payments in a current account in a day are covered on account of each other or there are no additional employees, and the same person is also the beneficial owner and representative of the other so-called group companies (i.e. also concludes transactions themselves), etc.;

[187] The FATF has defined the term 'shell company' in many of its guidelines as a company that does not have independent activities, notable assets, continuing business activities or employees, but it may also be a case of the activities of a shell company if, in addition to the aforementioned characteristics, a place of business is used that does not correspond to the conditions necessary for its activities, labour or other taxes are not paid, and there are large or rather large turnovers but no income seems to be earned from these. Obliged entities must keep in mind that several characteristics that refer to risks together or separately may be a sign of the use of a shell company or of other suspicious and unusual activity that does not refer to reasonable economic activities, in which case the obliged entities must also explain to Finantsinspektsioon within the meaning of points 4.3.6.7 and 4.4.2.10 of these Guidelines why the obliged entity has established a business relationship that corresponds to such characteristics and why it is continued.

vi. the person has just been established or they have no previous economic activities, but they declare unusually large transaction turnovers or unusual capacity;

vii. the person's transaction turnovers are unusually large and do not correspond to the customer's (representative's and beneficial owner's) experience, age and capacity to conclude such transactions, incl. the number of employees, and neither do the main transaction partners give reason to believe that the customer has the capacity for such transaction volumes;

viii. the person's ownership structure is complicated and not associated with the customer's economic activities, incl. the customer is not able to justify the selection;

ix. the person uses nominee directors[188] or nominee shareholders[189] in their management or ownership structure, whether it is formal or informal[190];

x. the person's jurisdiction is not associated with the customer's economic activities, incl. the customer is not able to justify the selection;

xi. the person's registration address is not associated with the customer's economic activities, incl. the customer is not able to justify the selection;

xii. the person's tax residency is not associated with the customer's economic activities, incl. the customer is not able to justify the selection;

xiii. the address of the person's place of business is located in an apartment building, is a post office box or in any other way inappropriate for operating in the relevant volume in the relevant area of activity;

xiv. the person wants to conclude large or relatively large transactions in the bank account or payment account, but the representatives or beneficial owners themselves do not want to establish financial relationships with the service provider;

xv. the activity volumes declared by the person do not correspond to those indicated in the annual report or do not correspond to transaction volumes that are reasonable in this area of activity;

xvi. the person's area of activity is basically an undetermined range of activities or the areas of activity that contradict each other or are completely different from each other;

xvii. the person wants a financial service that does not correspond to their usual profile, capacity or wishes that are probably real;

xviii. there is no information about or trace of the person on the Internet, although it should exist considering the volume of their planned transactions and area of activity;

xix. the person is unable to describe the objectives of the service they want or give explanations about their person (information required for the establishment of

[188] In English – nominee director.
[189] In English – nominee shareholder.
[190] For example, family members, business partners or other persons close to the beneficial owner, sometimes also called straw or front men.

identity, representative and beneficial owner and the purpose of the business relationship);

xx. the person logs in to the Internet bank solution from the same IP address used by other customers whilst the addresses of the places of business of the customers may not be the same and there may also be no other connections that would not make logging in from the same IP addresses unusual;

xxi. the person's beneficial owner or representative has also opened many other accounts where they are the representatives or beneficial owners without adequate explanations about why it is necessary to open so many accounts;

xxii. the person uses a changing IP address (the so-called Proxy service);

b. *the purpose of payments, i.e. what is going on in the current account* – the risks may be that (if one or several characteristics are present, depending on the situation):

i. incoming and outgoing payments do not match, i.e. the payments only move in one direction – 1) the person purchases goods that they never sell, 2) the person sells goods that they never purchase, 3) the person grants loans that are not repaid to them or are repaid without interest or the amount of the interest does not comply with the terms and conditions of the agreement, 4) the person repays a loan that they have never received;

ii. the outgoing payment transactions of the day are practically fully covered with the incoming transactions of the same day, i.e. the account balance is close to zero by the end of the day;

iii. transactions constantly take place between companies of the same group or between the same companies, who seem to be connected to each other;

iv. transactions take place in a manner where the funds move from one person (link) to another, whilst the use of links seems unusual and the first and last links of the chain could conclude transactions between each other as well;

v. the amounts of the payment transactions do not correspond to those declared upon the establishment of the business relationship (they are bigger), the volumes are increased (constantly) and this does not coincide with the customer's usual behaviour or capacity;

vi. the substance of the payment transactions is different than the activity declared by the customer;

vii. the customer constantly converts currencies, which may, among others, be economically harmful or have no reasonable purpose (currencies are constantly converted);

viii. the customer is not interested in transfer fees, constantly requests urgent payment and making transfers in such a manner is economically harmful and does not seem to correspond to the actual declarations of intent of the customer;

ix. incoming larger amounts are divided into smaller amounts as transfers or small amounts are collected and passed on as one large payment;

x. a small part of the incoming larger amounts, which are divided into smaller amounts as transfers, goes to natural persons, to the person who received the transfer (e.g. a transfer to the account holder's account in another bank or payment institution) or to other persons, which does not seem to have a reasonable economic purpose and the purpose of which seems to be a payment of a service fee for helping with possible concealment;

xi. incoming funds are constantly transferred in the same amount after a short period of time;

xii. the person does not make transfers for wages, utilities, taxes, etc. from the bank account or payment account;

xiii. the person has no employees or other resources (incl. warehouses, offices, etc.) for the provision of services and completing of the relevant transactions;

xiv. the purchased or sold goods are not transported and they are always received from the same port or ports of the same region (and, as an additional characteristic, this port is never paid any fees).

xv. the transport service provider is not paid for the transport of the purchased or sold goods or the person does not have the capability to transport goods themselves;

xvi. the transport of goods requires the existence of special equipment (e.g. refrigeration equipment) or the existence of special insurance contracts, but there are no signs that such equipment is used or insurance contracts have been entered into;

xvii. goods are transported across state borders where they have to be declared, but there are no customs documents, their content is illegible or not understandable, they only describe the loading of the goods and not transport, etc.;

xviii. goods are transported in a manner (incl. in packaging) that makes no sense;

xix. the quantities of goods are not consistent with the reasonable economic purpose or capacity, incl. the number of freight wagons, shipping containers, etc. does not correspond to reasonable economic capacity;

xx. the values of the goods or services declared by the transactions do not correspond to the actual values and they are under- or overvalued;

xxi. the values of transactions are figures that end with three or more zeros even though the value of the goods is given to the accuracy of a euro, ten cents or cent or the exact price of an item of goods is an amount that ends with three or four zeros;

xxii. signatures (and seals) have been copied onto the contracts that serve as a basis for the transaction, meaning that. they are placed under the text and are presented as images on the contract;

xxiii. the debt relationships that serve as a basis for the transactions are economically unreasonable or difficult to explain;

xxiv. the transactions on the bank account or payment account indicate that the account is used as a transit account;

xxv. irrespective of the size and repeated nature of transactions, it does not seem that income is earned from such activity or that this income is expressed in the balance of the account at the obliged entity;

xxvi. the activities of the customer or their counterparty indicate the provision of a financial service, but the respective authorisation is missing (e.g. provision of investment services, insurance services, payment services, etc.);

xxvii. e-money is constantly purchased;

xxviii. the persons send funds to other countries within the scope of occasional transactions (also considering the geographic risk), whereby the origin of the assets and the purpose of the transactions is unclear;

xxix. securities that do not circulate in the ordinary infrastructure of the securities market are purchased, sold or borrowed;

c. *the countries related to the payments* – the risks may be that the customers of financial institutions receive funds from or transfer funds to countries where the level of corruption is high, where the measures for money laundering and terrorist financing prevention are not adequate, which are in tax-free or low-tax regions, where the level of crime is high, etc., also the countries or the neighbouring countries of these countries, which are associated with a higher risk of terrorism, incl. are areas of conflict, or countries that have other important connections with the aforementioned countries;

d. *the manner in which the customer was found* – the risks may be that the customer was introduced to the obliged entity by a third party, in the case of whom there may be a conflict of interests between the customer and the obliged entity, because, in addition to the role of introducing, the third party also provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;

e. *the origin of the funds* – the risks may be that the funds used in a transaction are criminal proceeds or with an unusual origin or there is no reasonable economic explanation about their origin;

f. *the payment details* – the risks may be that the details of the payments made in the customer's current or payment account do not actually explain the content of the payments, e.g. transfer of funds, transfer, intercompany payment, loan return, return, etc., or the person transfers funds from their other account without an adequate explanation;

g. *the actual location of the customer* – the risks may be that the customer actually uses Internet banking solutions (IP address) in a country or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. are areas of conflict, or countries that have other important connections with the aforementioned countries;

2. in the case of securities transactions (purchase and sale, i.e. incl. so-called mirror transactions):

a. *the origin of the securities* – the risks may be that the origin of and the capacity to acquire the securities transferred by the customer to the securities account are unknown;

b. *the currency of transactions* – the risks may be that the customer buys or transfers securities to their securities account, which they purchased in one currency, and then sells them in another currency;

c. *the manner of completing transactions* – the risks may be that the customer buys and sells securities (incl. constantly) over the OTC market;

d. *the speed of the transaction* – the risks may be that the customer sells the securities immediately after buying them, incl. the transaction may be economically harmful;

e. *the economic justification of the transaction* – the risks may be that the customer sells securities (incl. constantly) whereas the transactions do not indicate that the customer cares about the income earned or that the customer concludes transactions that are economically justified;

f. *the duration of the investment* – the risks may be that the customer wants to sell a long-term investment early or a short period of time after making the investment;

g. *the repetition of transactions* – the risks may be that the customer repeatedly buys and sells securities without it having clear strategic or economic reasons;

h. *the manner in which the customer was found* – the risks may be that the customer was introduced to the obliged entity by a third party, in the case of whom there may be a conflict of interests between the customer and the obliged entity, because, in addition to the role of introducing, the third party also provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;

i. *the risk arising from the person of the customer with the appropriate differences, which are specified under the risk arising from the person of the customer in sub-point 1 of point 2 (layering);*

3. in the case of conversion of the funds in bank account and payment accounts into cash:

a. *the manner of completing the transaction* – the risks may be that cash is needed on account of the funds in the bank account or payment account by a person (service provider) who actually does this for a third party or the ultimate beneficial owner, whereas the activity of this service provider may correspond to the provision of payment services without them having the required licence, because funds are transferred to the service provider's current account, which are then converted into cash and thereafter delivered to the ultimate beneficial owner;

b. *the person who performs obligations* – the risks may be that a third party who specifically provides such cash-in-transit (CIT) services comes to collect the cash on behalf of the customer;

c. *the economic justification of the transaction* – the risks may be that the cash needs of the person that ultimately receives the cash are not justified or economically unreasonable;

d. *the manner in which the customer was found* – the risks may be that the customer was introduced to the obliged entity by a third party, in the case of whom there may be a conflict of interests between the customer and the obliged entity, because, in addition to the role of introducing, the third party also provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;

e. *the risk arising from the person of the customer with the appropriate differences, which are specified under the risk arising from the person of the customer in sub-point 1 of point 2 (layering);*

4. in the case of other financial services in general:

    a. *the duration of the contract* – the risks may be that the customer terminates the financial services contract before its expiry or does so repeatedly or consistently in the case of several contracts, incl. repays a loan immediately after taking it or repays it early in an unusual manner, an insurance contract is terminated after a short period of time or early in a manner that is unusual, fund units are sold immediately or after an unusually short period of time, purchased securities are sold immediately or after an unusually short period of time after their acquisition;

    b. *the transferability of the contract or obligations* – the risks may be that (i) the customer transfers their right or obligation arising from a contract repeatedly or in a short period of time after entry into the contract, (ii) with the aforementioned characteristic or separately transfers the contract to a third party without an obvious connection to the customer, (iii) information about the transfer is only given at the moment the right is exercised or the obligation is performed (e.g. information about the change in the beneficiary in the case of a life insurance contract is given immediately before or after the occurrence of a insured event);

    c. *the economic justification of the transaction* – the risks may be that the customer uses financial services or terminates them early, whilst the activity does not indicate that the customer cares about the loss made on the transaction or activity or economic justification;

    d. *the origin of the funds* – the risks may be that the source and origin of the funds used in the transaction cannot be identified or the explanation given about them is suspicious or unusual;

    e. *the location of the persons related to the contract in different countries* – the risks may be that the persons related to the contract are located in different countries (e.g. the policyholder, insured person and/or beneficiary in the case of a life insurance contract or the person who benefits from the contract in the case of other services and the location of the person who performs the financial obligation arising from the contract);

    f. *the person who performs obligations* – the risks may be that an obligation related to a financial service contract is performed by a third party or it is performed to an extent that does not correspond to the customer's usual capacity;

    g. *the manner in which the customer was found* – the risks may be that the customer was introduced to the obliged entity by a third party, in the case of whom there may be a conflict of interests between the customer and the obliged entity, because, in addition to the role of introducing, the third party also provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;

    h. *the risk arising from the person of the customer with the appropriate differences, which are specified under the risk arising from the person of the customer in sub-point 1 of point 2 (layering).*

3. Integration

Based on various threat assessments, typologies, the data accessible to Finantsinspektsioon, statistics, the observations made during on-site inspections and special information and considering the risks specific to Estonia, this phase of money laundering may be the following in the case of Estonia:

(i) funds are withdrawn from the bank account or payment account in cash (payment service) and integrated into the real economy;
(ii) the funds in a bank account or payment account are converted into cash;

(iii) a loan, the proceeds of a sale of fund units, the proceeds of a sale of an investment portfolio, an insurance indemnity, etc. are paid out to the customer in cash and these funds are integrated into the real economy;
(iv) cars, real estate or other assets are purchased for the funds in the bank account or payment account, through which the funds are integrated into the real economy (payment service).

Although the Know-Your-Customer principles is always applied upon the provision of financial services, i.e. the financial institution must always be convinced that it knows the customer, knows why the customer wants to receive the relevant financial service and knows that the customer's activities and conduct corresponds to the information known to the financial institution, in order to manage the risk of money laundering, the financial institutions should pay particular attention to the following in appropriate cases:

1. in the case of cash payments (points (i) to (iii)):

    a. *the capability of the customer to conclude such a transaction* – the risks may be that the cash withdrawal by the person concluding the transaction as a fact or the extent to which cash is withdrawn does not correspond to their ordinary capacity and needs or seems unusual and does not correspond to the agreements made between the parties;

    b. *the person who received funds in cash* – the risks may be that a third party, incl. a party that has no connection to the customer or that performs a payment service or a similar service for this purpose, although they do not have the relevant licence, receives funds in cash on behalf of the customer;

    c. *the nominal value of banknotes* – the risks may be that the customer withdraws most or a significant part of a larger amount in cash in large value banknotes (100, 200 or 500 euros or 100 dollars);

    d. *the manner in which the customer was found* – the risks may be that the customer was introduced to the obliged entity by a third party, in the case of whom there may be a conflict of interests between the customer and the obliged entity, because, in addition to the role of introducing, the third party also provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;

    h. *the risk arising from the person of the customer with the appropriate differences, which are specified under the risk arising from the person of the customer in sub-point 1 of point 2 (layering);*

    e. *any other relevant risks specified in point 2 (layering) (especially sub-point 1);*

2. in the case of purchases of goods for the funds in the bank account and payment account, *all relevant risks specified in point 2 (layering) (especially sub-point 1).*

Annex 2 – Terrorist financing risks and methods specific to Estonia

Terrorist financing is divided into three ways:

1. collection;
2. movement;
3. use of funds.

Terrorist financing does not only mean that the funds obtained in a legal or illegal manner are passed on for the commission of a specific act of terrorism (taking the terrorist to the place where the act of terrorism will be committed (flight tickets, etc.), acquisition of tools, equipment, etc. (weapons, explosives, etc.) for the commission of an act of terrorism). Transferring funds in order to strengthen terrorist organisations also means terrorist financing. The amounts meant for terrorist financing may be very small.

Although the risk/threat of terrorism is low in Estonia, this does not mean that Estonian financial institutions may not be used to finance terrorism. This Annex is based on different threat assessments, typologies, data accessible to Finantsinspektsioon, statistics, observations made during on-site inspections and special information. This takes into account the services and products offered by financial institutions and their volumes, and the geographic location of Estonia. The biggest threats in Estonia may be related to collection (special non-profit associations and foundations) and movement, but the use of funds (international sanctions) must also be given attention.

The biggest threat in Estonia is related to the manner of movement, where the funds received as a result of criminal activities or in legal ways are given orders for the performance of transfers in bank account or payment accounts (point (i) of movement).

Below is a list of products, services and ways through which Estonian financial institutions may primarily (this is not an exhaustive list) be abused for the purposes of terrorist financing and to which financial institutions should therefore give special attention. This overview is limited only to the financial institutions under the supervision of Finantsinspektsioon (credit institutions, fund management companies, investment firms, life insurance undertakings, payment institutions, creditors and credit intermediaries) and the products and services primarily offered by these financial institutions have been taken into account.

Some of the indicators listed in this Annex may also occur alone or together in ordinary or legitimate transactions, which is why the provided non-exhaustive list must be taken as a list that helps to identify the risks associated with the prevention of money laundering and terrorism.

1. Collection

Based on various threat assessments, typologies, the data accessible to Finantsinspektsioon, statistics, the observations made during on-site inspections and special information and considering the risks specific to Estonia, this way of terrorist financing may be the following in the case of Estonia:

(i) a customer that is a non-profit association or a foundation deposits, collects or raises funds or other assets, which are then sent to terrorists or terrorist organisations;
(ii) a customer that is not a non-profit association or a foundation deposits, collects or raises funds or other assets, which are then sent to terrorists or terrorist organisations.

Although the Know-Your-Customer principles is always applied upon the provision of financial services, i.e. the financial institution must always be convinced that it knows the customer, knows why the customer wants to receive the relevant financial service and knows that the customer's activities and conduct corresponds to the information known to the financial institution, in order to manage the risk of terrorist financing, the financial institutions should pay particular attention to the following in appropriate cases:

1. in the case of a service provided to non-profit associations and foundations:

    a. *the operating region of the non-profit association and foundation* – this is probably the most important indicator and may be related to the operating region being connected to countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. are areas of conflict, or countries that have other important connections with the aforementioned countries;

    b. *the purpose of the assets collected by the non-profit association and foundation* – the risks may be that funds or other assets are collected for persons, groups, organisations, etc. who are related to countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. are areas of conflict, or countries that have other important connections with the aforementioned countries;

    c. *the objectives of the non-profit association and foundation in general* – the risks may be that funds or other assets are collected for persons, groups, organisations, etc. who collect funds or other assets themselves for persons, groups and organisations, etc. that are related to countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. are areas of conflict, or countries that have other important connections with the aforementioned countries;

    d. *cash deposits or withdrawals* – the risks may be that a non-profit association or foundation constantly or once deposits cash in a bank account or payment account or withdraws it whilst such activity does not correspond to the activities expected from the non-profit association or foundation;

    e. *the other relevant risks highlighted under transfers made from bank account and payment accounts in point 2 (movement), incl. the risk arising from the person of the customer;*

2. in the case of provision of services to other persons:

    a. *their legal form* – the risks may be that the customer's actual objective is to collect funds, but the legal form of the customer does not reflect this activity or the customer tries to hide their actual activity in any other manner;

    b. *all circumstances with the relevant differences arising from the person, which are highlighted in point 1 (collection) under the services provided to non-profit associations and foundations.*

2. Movement

Based on various threat assessments, typologies, the data accessible to Finantsinspektsioon, statistics, the observations made during on-site inspections and special information and considering the risks specific to Estonia, this way of terrorist financing may be the following in the case of Estonia:

(i) the customer concludes transactions in the bank account or payment account (so-called payment service), the purpose of which is to transfer funds, irrespective of the contract serving as a basis therefor, i.e. the legal relationship (considering the specific circumstances of Estonia, this is the most likely manner to which financial institutions must therefore give special attention);

(ii) the customer gives orders regarding funds they have received as a loan, upon the realisation of an insured risk, sale of fund units or as a result of securities transactions or the realisation of a securities portfolio.

Although the Know-Your-Customer principles is always applied upon the provision of financial services, i.e. the financial institution must always be convinced that it knows the customer, knows why the customer wants to receive the relevant financial service and knows that the customer's activities and conduct corresponds to the

information known to the financial institution, in order to manage the risk of terrorist financing, the financial institutions should pay particular attention to the following in appropriate cases:

1. in the case of transfers made from bank account and payment accounts:

    a. *the risk arising from the person of the customer* – the risks may be that (if one or several characteristics are present, depending on the situation):

        i. the person is a politically exposed person;

        ii. the person has or seems to have a connection to countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. areas of conflict, or countries that have other important connections with the aforementioned countries;

        iii. the person has no connection with Estonia, but they still want to receive the service in Estonia;

        iv. the person was established or originally from one country (e.g. address of the place of business), their beneficial owner is originally from another country (e.g. address of the place of residence), the current account has been opened in a third country and transactions are concluded with persons not associated with these countries (said conditions do not have to be present at the same time);

        v. the person carries out large transactions, whilst the representative and beneficial owner of the customer is the same person, incl. this person logs in to Internet bank solutions to conclude transactions themselves, and additional circumstances that are present may be that the incoming and outgoing payments in a current account in a day are covered on account of each other or there are no additional employees, and the same person is also the beneficial owner and representative of the other so-called group companies (i.e. also concludes transactions themselves), etc.;

        vi. the person has just been established or they have no previous economic activities, but they declare unusually large transaction turnovers or unusual capacity;

        vii. the person's transaction turnovers are unusually large and do not correspond to the customer's (representative's and beneficial owner's) experience, age and capacity to conclude such transactions, incl. the number of employees, and neither do the main transaction partners give reason to believe that the customer has the capacity for such transaction volumes;

        viii. the person's ownership structure is complicated and not associated with the customer's economic activities, incl. the customer is not able to justify the selection;

        ix. the person's jurisdiction is not associated with the customer's economic activities, incl. the customer is not able to justify the selection;

        x. the person's registration address is not associated with the customer's economic activities, incl. the customer is not able to justify the selection;

        xi. the person's tax residency is not associated with the customer's economic activities, incl. the customer is not able to justify the selection;

xii. the address of the person's place of business is located in an apartment building, is a post office box or in any other way inappropriate for operating in the relevant volume in the relevant area of activity;

xiii. the person wants to conclude large or relatively large transactions in the bank account or payment account, but the representatives or beneficial owners themselves do not want to establish financial relationships with the service provider;

xiv. the activity volumes declared by the person do not correspond to those indicated in the annual report or do not correspond to transaction volumes that are reasonable in this area of activity;

xv. the person's area of activity is basically an undetermined range of activities or the areas of activity that contradict each other or are completely different from each other;

xvi. the person wants a financial service that does not correspond to their usual profile, capabilities or wishes that are probably real;

xvii. there is no information about or trace of the person on the Internet, although it should exist considering the volume of their planned transactions and area of activity;

xviii. the person is unable to describe the objectives of the service they want or give explanations about their person (information required for the establishment of identity, representative and beneficial owner and the purpose of the business relationship);

xix. the person logs in to the Internet bank solution from the same IP address used by other customers whilst the addresses of the places of business of the customers may not be the same and there may also be no other connections that would not make logging in from the same IP addresses unusual;

xx. the person's beneficial owner or representative has also opened many other accounts where they are the representatives or beneficial owners without adequate explanations about why it is necessary to open so many accounts;

xxi. the person uses a dynamic IP address (the so-called Proxy service);

b. *the countries related to the payments* – this is probably the most important indicator and may be related to the customers of financial institutions receiving funds from or transferring funds to countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. are areas of conflict, or countries that have other important connections with the aforementioned countries;

c. *the origin of the funds* – the risks may be that the funds used in a transaction are criminal proceeds;

d. *the purpose of the payments* – the risks may be that the transactions are related to the provision of various aid and donations to countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. are areas of conflict, or countries that have other important connections with the aforementioned countries, and this is done either directly or via non-profit associations or foundations, or when the purpose is to

purchase food for other people once or constantly, pay for transport services or other unusual kind of aid;

e. *the payment details* – the risks may be that the transactions in the customer's bank account and payment account are explained as donation, *sadaqa, zakat, zaakat, Ramadan, Eid al-Adha, iftar, Eid al-Fitr, hajj,* sponsor aid or as other similar aid;

f. *the nature of the purchased or sold product or service* – the risks may be that the product or service purchased or sold by the transaction can be used for committing an act of terrorism;

g. *the risk related to the origin of the customer* – the risks may be that the customer, the persons related to them (representatives, beneficial owners, etc.) or persons known to be connected to these persons are originally from or their place of residence or location is in a country or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. are areas of conflict, or countries that have other important connections with the aforementioned countries;

h. *the actual location of the customer* – the risks may be that the customer actually uses Internet banking solutions (IP address) in a country or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. are areas of conflict, or countries that have other important connections with the aforementioned countries;

i. *the activities of the customer* – the risks may be that the customer or the persons related to them have a connection to countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. areas of conflict, or countries that have other important connections with the aforementioned countries and the risk may constitute the sale or purchase of products and services to or from such countries;

j. *the counterparty risk of the customer* – the risks may be that the customer's transaction partner is in one way or another (incl. sells products, is originally from, registered or established in, etc.) connected to countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. areas of conflict, or countries that have other important connections with the aforementioned countries;

k. *the other activities of the customer* – the risks may be that the other activities of the customer or the persons related to them (representatives, beneficial owners, etc.) are known to be connected to countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. are areas of conflict, or countries that have other important connections with the aforementioned countries;

l. *the currency used* – the risks may be that a currency is used in transactions that is used in the countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. areas of conflict, or countries that have other important connections with the aforementioned countries;

m. *the manner in which the customer was found* – the risks may be that the customer was introduced to the obliged entity by a third party, in the case of whom there may be a conflict of interests between the customer and the obliged entity, because, in addition to the role of introducing, the third party also provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;

n. *currency conversion* – the risks may be that the customer constantly converts currencies, which may, among others, be economically harmful or have no reasonable purpose (currencies are constantly converted);

2. in the case of other services and transactions whereby orders are given to funds:

    a. *the connection of the customer to the recipient of the transfer* – the risk may be that the customer gives orders regarding funds they have received as a loan, upon the realisation of an insured risk, sale of fund units or as a result of securities transactions or the realisation of a securities portfolio and wants to send these funds to a third party, incl. to a person to whom the customer is not connected;

    b. *the other relevant risks highlighted under transfers made from bank account and payment accounts in point 2 (movement).*

3. Use of funds

Based on various threat assessments, typologies, the data accessible to Finantsinspektsioon, statistics, the observations made during on-site inspections and special information and considering the risks specific to Estonia, this way of terrorist financing may be the following in the case of Estonia:

(i) the customer withdraws funds from a bank account or payment account in cash;
(ii) the customer concludes other transactions that are actually covered under 'movement', but need to be separately highlighted in the case of use of funds, for example, to purchase food for other people once or constantly, pay for transport services or provide other unusual kind of aid.

Although the Know-Your-Customer principles is always applied upon the provision of financial services, i.e. the financial institution must always be convinced that it knows the customer, knows why the customer wants to receive the relevant financial service and knows that the customer's activities and conduct corresponds to the information known to the financial institution, in order to manage the risk of terrorist financing, the financial institutions should pay particular attention to the following in appropriate cases:

1. in the case of cash withdrawal from bank account and payment accounts:

    a. *the place where cash is withdrawn* – the risks may be that the customer withdraws cash in the countries or the neighbouring countries of the countries that are associated with a higher risk of terrorism, incl. are areas of conflict, or countries that have other important connections with the aforementioned countries;

    b. *the nominal value of banknotes* – the risks may be that the customer withdraws most or a significant part of a larger amount in cash in large value banknotes (100, 200 or 500 euros or 100 dollars);

    c. *the other relevant risks highlighted under transfers made from bank account and payment accounts in point 2 (movement);*

2. in the case of transfers made from bank account and payment accounts:

    a. *the purpose of payments* – the risks may be that the purpose is to purchase food for other people once or constantly, pay for transport services or other unusual kind of aid;

    c. *the other relevant risks highlighted under transfers made from bank account and payment accounts in point 2 (movement), incl. the risk arising from the person of the customer.*

Comprehensive obligation

As the risk/threat of terrorism is low in Estonia, the Estonian financial institutions must primarily consider, in the case of the above, the implementation of international sanctions, which in most cases requires not making

funds accessible, i.e. (i) the customer of the financial institution or a related person is a subject of an international sanction, or (ii) an attempt is made to transfer funds to such a person or to make the funds accessible in any other manner.