



Finantsinspeksioon

**Advisory Guidelines of the Finantsinspeksioon
'Organisational approaches and preventive measures of credit and financial institutions for prevention of
money laundering and terrorist financing'**

The advisory guidelines have been established by Resolution No. 1.1-7/172 of the management board of the Finantsinspeksioon of 26 November 2018 and amended by Resolution No. 1.1-7/58 of the Management Board of the Finantsinspeksioon of 8 April 2024

TABLE OF CONTENTS

1.	Competence of Finantsinspeksioon	4
2.	Purpose, scope of application, underlying principles and definitions.....	4
2.1.	Objective.....	4
2.2.	Scope of application.....	4
2.3.	Underlying principles and definitions.....	5
3.	Organisational structure and risk management.....	7
3.1.	General principles	7
3.2.	Risk assessment	9
3.3.	Risk appetite	11
3.4.	Activities of the management board.....	13
3.5.	Appointing the responsible member of the management board, their functions and role	15
3.6.	Activities of the supervisory board.....	16
3.7.	Building the organisation by the three lines of defence principle.....	17
3.7.1.	General principles.....	17
3.7.2.	First line of defence	19
3.7.3.	Second line of defence, including the function of the compliance officer.....	20
3.7.4.	Third line of defence.....	27
3.8.	Business continuity and events of operational and reputational risk	28
3.9.	Training.....	28
3.10.	Establishment of and requirements for rules of procedure	29
3.11.	Risk management and measures in a group.....	31
4.	Due diligence measures in respect of customers or third parties	35
4.1.	General principles	35
4.2.	Risk-based approach upon the application of due diligence measures	39
4.3.	Due diligence measures upon the establishment of business relationships	42
4.3.1.	Identification of a natural person and representative.....	42
4.3.2.	Identification of a legal entity.....	50
4.3.3.	Identification of the beneficial owner of a legal entity	54
4.3.4.	Identification of a politically exposed person	57
4.3.5.	Identification of the source and/or origin of wealth.....	61
4.3.6.	Identification of the purpose and nature of a business relationship or occasional transaction 61	
4.4.	Due diligence measures during the business relationship	66
4.4.1.	Updating data.....	66
4.4.2.	Business relationship monitoring	67
4.4.3.	Identification of the source and origin of funds used in a transaction	72
4.5.	Simplified due diligence measures.....	74

4.6.	Enhanced due diligence measures.....	75
4.7.	Special cases of due diligence measures.....	76
4.7.1.	Due diligence measures applied to life insurance undertakings.....	76
4.7.2.	Due diligence measures applied to creditors and credit intermediaries	78
4.7.3.	Due diligence measures applied to fund management companies	79
4.8.	Due diligence measures applied by another person	79
4.8.1.	Outsourcing.....	79
4.8.2.	Relying on a third party	82
4.8.3.	Failure to apply due diligence measures to ultimate beneficial owners in correspondent relationships	82
4.9.	Relationships with other credit or financial institutions and shell institutions.....	83
4.10.	Transactions with natural persons and legal entities operating in high-risk third countries, including FATF high-risk countries	85
5.	Registration and retention of data	86
6.	Refusal to establish a business relationship and conclude a transaction and (extraordinary) cancellation of a business relationship	88
6.1.	Refusal to establish a business relationship or conclude a transaction	88
6.2.	Postponement of a transaction.....	89
6.3.	(Extraordinary) cancellation of a business relationship.....	90
7.	Obligation to report to the Financial Intelligence Unit.....	91
8.	Forwarding of information related to payer and payee	93
9.	Obligation to implement due diligence measures again	93
10.	Implementation of the Guidelines	94
	Annex 1 – Stages, typologies and risk indicators of money laundering	
	Annex 2 – Stages and risk indicators of terrorist financing	

1. Competence of Finantsinspeksioon

- 1.1. Pursuant to § 3 of the Financial Supervision Authority Act (hereinafter the FSAA), Finantsinspeksioon (the Financial Supervision Authority, hereinafter the FSA) conducts state financial supervision in order to enhance the stability, reliability, transparency and efficiency of the financial sector, reduce systemic risks and 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 Act¹ (hereinafter the MLTFPA), the FSA 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. The FSA exercises supervision pursuant to the procedure provided in the FSAA, taking into account the specifications provided in the MLTFPA.
- 1.3. Pursuant to subsection 57 (1) of the FSAA, the FSA has the right to issue advisory guidelines to explain legislation regulating the activities of the financial sector and provide guidance to subjects of financial supervision.

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

2.1. Objective

- 2.1.1. The purpose of these advisory guidelines (hereinafter the Guidelines) is to contribute to increasing the ability of obliged entities² 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. The Guidelines explain the content and fulfilment of the requirements established in the MLTFPA and the directly related legislative acts³ to the obliged entities as well as the understanding of the risks associated with service provision. The Guidelines also guide the obliged entities in the establishment and operation of the organisational solution required for the management of the risks of money laundering and terrorist financing prevention.
- 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 upon compliance with the requirements stipulated in the MLTFPA and that are subject to supervision by the FSA⁴ (hereinafter the obliged entity). Such entities are:

¹ Money Laundering and Terrorist Financing Prevention Act. – RT I, 10.02.2023, 30

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 the FSA are determined by the FSAA.

- 2.2.1.1. credit institutions⁵;
- 2.2.1.2. payment institutions⁶;
- 2.2.1.3. e-money institutions⁷;
- 2.2.1.4. insurance undertakings⁸;
- 2.2.1.5. insurance brokers⁹;
- 2.2.1.6. fund management companies and investment funds established as public limited companies¹⁰;
- 2.2.1.7. investment firms¹¹;
- 2.2.1.8. creditors and credit intermediaries¹²;
- 2.2.1.9. Estonian branches (establishments) of foreign credit and financial institutions that provide the service stipulated in points 2.2.1.1 to 2.2.1.8¹³;
- 2.2.1.10. a central securities depository¹⁴.

2.2.2. The FSA 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. The FSA 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.

2.3. Underlying principles and definitions

2.3.1. The terms as used in the Guidelines have been defined in Division 2 of Chapter 1 of the MLTFPA, Section 1 of Chapter I of Directive (EU) 2015/849 of the European Parliament and of the Council¹⁵

⁵ Within the meaning of Article 4(1)(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, 27.06.2013, pp 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 Obligated Entities, the only payment service providers subject to supervision by the FSA 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 that 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 that 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 that 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 the option stipulated in subsection 27 (1) of the MLTFPA to open an account, including a securities account, before the application of due diligence measures where transactions cannot be made by the customer or in the name of the customer with the property held in the account until the full application of the due diligence measures specified in clauses 20 (1) 1) to 3), thereby applying the due diligence measures as soon as reasonably possible.

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.

(hereinafter AMLD 4), Directive 2018/843 of the European Parliament and of the Council¹⁶ (AMLD 5), the glossary of FATF Recommendations 2012¹⁷ and FATF Methodology 2013¹⁸ or the guidelines and other guidance materials of the European Banking Authority (hereinafter the EBA). If there is no management board, the provisions concerning the management board apply to the 'director of a branch'.

- 2.3.2. Compliance with the money laundering and terrorist financing prevention requirements comprises, within the meaning of the Guidelines, all of the activities that the FATF expects from member states and obliged entities in the application of preventive measures, including prevention of corruption and prevention of the proliferation of weapons of mass destruction¹⁹.
- 2.3.3. The requirements arising from effective legislation²⁰, international practice and the legislation directly related to the MLTFPA, the other advisory guidelines of the FSA and the guidelines and other guidance materials of the EBA²¹ must be taken into account upon the implementation of the Guidelines.
- 2.3.4. In the case of mandatory 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 is hereinafter also 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, including 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, including risks associated with outsourcing;
 - 2.3.5.4. the risks related to states or geographic regions or jurisdictions, including presence in other countries or provision of services to cross-border customers from a distance.

Online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849>. (21.07.2023)

¹⁶ Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. Online: <https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32018L0843>. (21.07.2023)

¹⁷ The FATF Recommendations 2012 (last updated on February 2023). Online: <http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html>. (21.07.2023)

¹⁸ The FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems 2013 (last updated in October 2021). Online: <http://www.fatf-gafi.org/publications/mutualevaluations/documents/fatf-methodology.html>. (21.07.2023)

¹⁹ In English – Financing of proliferation. See FATF Recommendation 7 for additional explanations for financing of proliferation of weapons of mass destruction, whereby prevention of proliferation of weapons of mass destruction primarily refers to the preparation, acquisition, development, export, reloading, mediation, carriage, storage or use of nuclear, chemical or biological weapons or other material means for the production of said weapons.

²⁰ This includes the general guidance materials concerning the organisation and activities of financial institutions.

²¹ As the relevant documents (e.g. the EBA Guidelines) and the requirements contained therein are constantly changing, the most up-to-date documents and requirements, which may differ from those set out in this version of the Guidelines at any given time, should always be taken into account when applying the Guidelines.

An obliged entity places the above in the context of the risks highlighted by supervision authorities²², law enforcement agencies and the state that threaten Estonia²³ as well as in the context of the European Union risks identified by the institutions of the European Union²⁴ considering the size of the obliged entity on the 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 arising from their activities etc., the more frequently the measures described in the Guidelines must be implemented or the more extensive the measures must be.

- 2.3.6. In the case of problems in the application or 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 the 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, which means that the obliged entity must be able to justify, where necessary, why they do not implement some points of the Guidelines or implement them only partially.
- 2.3.8. It may be necessary to apply measures differing from the Guidelines or additional measures under certain circumstances in order to identify and manage money laundering and terrorist financing risks, which is why an obliged entity cannot justify non-compliance with legislation simply with the fact that they followed these Guidelines word-for-word.
- 2.3.9. In the case of questions related to the prevention of money laundering and terrorist financing, the obliged entity will not remove themselves in the communication with the customer. Where necessary, the obliged entity must explain to the customer the necessity of the requirements in the public interest. For this purpose, the obliged entity creates customer service solutions in such a manner that the requirements arising from legislation and the Guidelines are built into the solutions as well as possible, thereby guaranteeing the smoothest customer service solution possible while complying with the obligations arising from legislation and the Guidelines.

3. Risk management and organisational structure

3.1. General principles

- 3.1.1. The organisational structure of the obliged entity must be such as to effectively prevent money laundering and terrorist financing.
- 3.1.2. The prevention of money laundering and terrorist financing are separate risk management areas. The management of these risks must be part of the overall governance of the obliged entity's organisation and risk management system.
- 3.1.3. The management board of the obliged entity represents the culture of money laundering and terrorist financing prevention. The management board guarantees 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 that the relevant risk considerations are taken into account to a suitable extent in the decision-making processes of the obliged entity.
- 3.1.4. The risk management of the obliged entity must comply with the principle of proportionality, i.e.

²² For example, possible money laundering and terrorist financing risk assessments by the FSA and the Financial Intelligence Unit (FIU), the FIU Yearbook, typology reports, etc.

²³ For example, the National Risk Assessment (NRA), where the money laundering and terrorist financing risks of Estonia are assessed.

²⁴ For example, the risk assessment of the European Commission, i.e. the Supranational Risk Assessment (SNRA).

the size of the obliged entity's organisation, the nature, scope and level of complexity of the activities and services provided, including the risk appetite and risks arising from activities of the obliged entity. The objective is to achieve the effectiveness of regulations and the protection of the Estonian financial system and economic space against money laundering and terrorist financing, thereby ensuring the credibility of the business environment.

- 3.1.5. A managing body of the obliged entity²⁵ is responsible for approving the obliged entity's money laundering and terrorist financing prevention strategy and supervision of its implementation. This requires sufficient knowledge, skills and experience to understand the risks of money laundering and terrorist financing related to the activities and business model of the obliged entity, including knowledge of the Estonian legal framework related to the prevention of money laundering and terrorist financing.
- 3.1.6. In order to comply with the obligations set out in the MLTFPA, the obliged entity must assess:
- i. the risk of money laundering and terrorist financing arising from the nature and level of complexity of the activity (risk assessment of all activities);
 - ii. the risk of money laundering and terrorist financing arising from the establishment of business relationships or occasional transactions (individual risk assessments for determining the risk profile and risk level of a customer or transaction).
- 3.1.7. Each risk assessment must consist of two separate but related stages:
- i. identification of risk factors of money laundering and terrorist financing, i.e. variables which, alone or in combination, may increase or reduce the risk of money laundering and terrorist financing
 - ii. assessment of the risk of money laundering and terrorist financing
- 3.1.8. In managing risks, the obliged entity must strike a balance between financial inclusion and the measures implemented to mitigate the risks of money laundering and terrorist financing in order to avoid persons being unduly deprived of legitimate access to financial products and services due to a higher risk of money laundering or terrorist financing.²⁶ For this purpose, the obliged entity may, *inter alia*:

²⁵ As defined in the EBA document of 14.06.2022 'Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849' issued as advisory guidelines of the FSA on the basis of Resolution No. 1.1-7/182 of the management board of the FSA of 21.11.2022. Online: <https://www.fi.ee/et/juhendid/pangandus-ja-krediit/euroopa-pangandusjarelevalve-suuniste-suuniste-direktiivi-el-2015849-artikli-8-ja-vi-peatuki-kohase>. (21.07.2023).

²⁶ Unjustified de-risking ('risk reduction' is also used in EBA Guidelines). See, *inter alia*, EBA 31.03.2023 'Guidelines on policies and controls for the effective management of ML/TF risks when providing access to financial services', issued as advisory guidelines of the FSA on the basis of Resolution No. 1.1-7/154 of the Management Board of the FSA as of 9 October 2023, applicable as of 3 November 2023. Herein also referred to as the EBA Guidelines on policies and controls for the effective management of AML risks when providing access to financial services. Online: <https://www.fi.ee/sites/default/files/2023-10/pp%20nr%2005%20EBA%20deriskimise%20suuniste.pdf>. These guidelines and the related point 3.1.8 of the Guidelines apply to both credit and financial institutions in the provision of services in general. In this context, companies and other customers who are not protected under the basic payment service institute are also protected against unlawful risk reduction under the guidelines. The requirements for the management of money laundering and terrorist financing risks in the narrower context of the provision and refusal to provide basic payment services are discussed in more detail in the FSA's advisory guideline 'Requirements for providers of basic payment services'. Established by Resolution No. 1.1-7/195 of the Management Board of the FSA of 4 December 2023. Online: https://www.fi.ee/sites/default/files/2023-12/Finantsinspeksiooni%20soovituslik%20juhend%20N%C3%B5uded%20p%C3%B5himakseteenuste%20osutajatele_kinnitustud.pdf.

- i. adjust the level and intensity of controls²⁷ according to the money laundering and terrorism risk posed by a particular customer;
 - ii. provide the customer with basic financial products and services²⁸ in order to legitimately limit the possibility of using products and services with a higher risk of money laundering or terrorist financing and to detect unusual transactions and transaction patterns, including the misuse of products and services, more easily. Such restrictions must be necessary and proportionate and must not unreasonably prevent a customer from accessing financial products and services;
 - iii. consider other options and measures to mitigate a higher risk of money laundering and terrorist financing before refusal to establish a business relationship, termination of a business relationship or refusal of a transaction in order to avoid persons being unduly deprived of legitimate access to financial products and services.
- 3.1.9. 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, allowing them to comply fully with the provisions of legislation and the Guidelines and the expected accuracy according to the scope of their duties. In addition, they must have passed the respective training for this or received instructions from the obliged entity in any other manner.

3.2. Risk Assessment

- 3.2.1. An obliged entity prepares and regularly updates its 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 methods 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 impediments (i.e. its vulnerability)²⁹.
- 3.2.2. The content of the risk assessment and its thoroughness, and the regularity of its updating, depend on the size of the obliged entity, the nature, scope and level of complexity of its activities and services, and the risks associated with the activities of the obliged entity.
- 3.2.3. The results of the National Risk Assessment are taken into account when deciding on the regularity of at which the risk assessment is updated. 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

²⁷ For example, monitoring a business relationship.

²⁸ According to Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features (hereinafter the Payment Account Directive), which was transposed into the Estonian law with the Law of Obligations Act (hereinafter the LOA, Chapter 40, Division 2), credit institutions are required to enter into contracts with consumers for the provision of payment services.

Pursuant to clause 35 (1) 6) of the MLTFPA, basic payment services relating to a liability account are deemed factors reducing the risks of money laundering and terrorist financing. The provision of basic payment services may be refused upon the establishment and duration of a business relationship for reasons of money laundering or terrorist financing prevention in the cases and under the conditions specified in legislation (in particular the LOA, subsection 42 (1) of the MLTFPA, the Payment Account Directive), taking into account the guidelines of the FSA on ensuring the accessibility of basic payment services referred to in footnote 26. This means that a service corresponding to the content of the basic payment service may also be provided to a wider range of persons outside the basic payment service institution as long as this ensures that the legitimate objectives of financial inclusion are achieved.

²⁹ For example, where 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.

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.

3.2.4. The obliged entity must be prepared to justify their risk handling, including the grounds for taking and refusing to take risks, to the competent supervisory authority.

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

3.2.5.1. At first, the obliged entity identifies the risks/threats arising from their activities, in addition to 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, assessed and analysed specifically as at the time the risk assessment is carried out and 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 categories:

- i. the risk related to customers, i.e. both specific customers and customer categories
- ii. product, service or transaction risk, including new and/or future product, service or transaction³⁰ risk
- iii. the risk related to the communication or mediation channels between the obliged entity and customers³¹ or to channels for the transmission and sale of products, services or transactions, including such new and/or future channels³² (hereinafter also the marketing channels)
- iv. risk related to countries or geographic regions or jurisdictions

3.2.5.2. The obliged entity determines the areas with the smaller and larger money laundering and terrorist financing risk, the risk appetite and the risk management model (compensation mechanisms) for the mitigation of the risks/threats arising from their activities and identifies the residual risk as well as its size and impact on the obliged entity after the implementation of the compensation mechanisms. The size of the maximum risk/threat associated with activities, i.e. the situation where the obliged entity should take risks to the maximum extent permitted with the risk appetite, excluding the case specified in point 3.4.3.4 of the 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 management of the risks to be taken, but also, among other things, the measures implemented with capital or other liquid resources, etc.

3.2.5.3. The obliged entity must obtain information from a number of sources to identify money laundering and terrorist financing risks, which is accessible individually or through available tools or databases combining information from several sources. In assessing the risks, the obliged entity must take into account, among other things, the risk and threat assessments of the Estonian state and the European Union, the European Commission's list of high-risk third countries, information from the FIU, governmental and competent supervisory authorities, and information gathered during the initial due diligence process and ongoing business relationship monitoring.

3.2.5.4. The risk assessment must cover all of the business activities and the initial level of customer due diligence that the obliged entity applies in specific situations and to specific types of customers, products, services and transmission channels. Individual risk assessments provide

³⁰ 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.

³¹ IT channels and channels that require physical contact must all be taken into account.

³² The money laundering and terrorist financing risk of new and/or future communication or mediation channels or transmission channels of products, services or transactions must be assessed as a part of product governance.

information but are not a substitute for a risk assessment that covers all of the business activities.

- 3.2.5.5. The measures of risk management with which significant changes in the risks arising from the activities of the obliged entity are identified within a reasonable time are determined in the risk assessment document.
- 3.2.6. 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.
- 3.2.7. If the obliged entity is, as the parent company, a part of a larger group that provides financial services, the risk assessment document, including the risks/threats affecting the activities of the obliged entity and the compensation mechanisms, must reflect the circumstances associated with the entire group³³ (including 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.
- 3.2.8. 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 in³⁴ other countries or regions (including in the case of provision of a cross-border service and concentration on serving certain customer groups³⁵), the risk assessment document must also reflect the risks specified in point 3.2.5.1 associated with these countries or territories.
- 3.2.9. When preparing and updating the risk assessment, the obliged entity must take into account, *inter alia*, the relevant EBA Guidelines (including the EBA Guidelines on risk factors³⁶) and assessments.
- 3.2.10. The risk assessment document is established and approved in writing by the management board of the obliged entity by its resolution.

3.3. Risk appetite

- 3.3.1. The obliged entity prepares and regularly updates the risk appetite³⁷ document. The risk appetite document determines the risk levels and types that are primarily associated with the higher-than-usual threat that a customer may perform transactions deviating from their ordinary activities³⁸, including 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.
- 3.3.2. The risk appetite document determines the set of risk levels and types that the obliged entity is

³³ A group within the meaning of this point is restricted only to companies that provide financial services.

³⁴ The term 'originating in' 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.

³⁵ Within the meaning of this footnote, 'originating in' means the connection selected by the obliged entity itself, including 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.

³⁶ EBA 01.03.2021 'Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions under Articles 17 and 18(4) of Directive (EU) 2015/849, repealing and replacing guidelines JC/2017/37', issued as advisory guidelines of the FSA on the basis of Resolution No. 1.1–7/160 of the FSA management board of 27.09.2021. Online: <https://www.fi.ee/et/juhendid/pangandus-ja-krediit/euroopa-pangandusjarelevalve-suunis-suunised-mis-koostatud-direktiivi-el-2015849-artikli-17-ja>. (21.07.2023)

³⁷ 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. The definition of risk is set out in § 10 of the MLTFPA.

³⁸ A customer, product and service or another circumstance that in the opinion of the obliged entity requires more frequent actions for the purpose of managing the risk of money laundering or terrorist financing and that is 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 is, 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.

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.

- 3.3.3. The regularity at which the risk appetite is updated depends on the size of the obliged entity, the nature, scope and level of complexity of its activities and services, including the risks associated with the activities of the obliged entity. The risk must be reviewed, *inter alia*, if the obliged entity identifies changed or additional risks in its activities when carrying out the risk assessment. Also if 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, transformation of the organisation, changes in the structure and volume of services, expansion of the customer base, diversification of services, etc.).
- 3.3.4. The content of the risk appetite document and its thoroughness depend on the size of the obliged entity, the nature, scope and level of complexity of its activities and services, including the risks associated with the activities of the obliged entity. Also 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. The risk assessment document must clearly show that the risk assessments of the Estonian state and the European Union, *inter alia*, have been taken into account in its preparation.
- 3.3.5. 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 other³⁹.
- 3.3.6. The risk appetite document must include at least the following:
 - 3.3.6.1. The obliged entity determines the risks (measurable) at the qualitative and quantitative levels, including 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, thereby also taking into account point 3.3.8. Among other things, the risk appetite document must include whether and to what extent the obliged entity intends to establish business relationships with entities from states outside the European Economic Area and which services and via which sales channels they are prepared to provide to them.
 - 3.3.6.2. The obliged entity also determines the compensation mechanisms (measured) at the qualitative and quantitative levels for the mitigation of the risks taken. The document must explain how the specific mechanisms mitigate the risks. 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, excluding in the cases specified in point 3.4.3.4 of the Guidelines. The compensation mechanisms are primarily the establishment of an appropriate organisational solution for the management of the risks to be taken, but also, among other things, the measures implemented with capital or other liquid resources, etc.
 - 3.3.6.3. The risk management measures are 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). Also the situations where compensation mechanisms are not commensurate with the risk appetite (i.e. the obliged entity can no longer tolerate the risks it has taken or will take) and

³⁹ 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.

measures to respond to such circumstances.

- 3.3.7. In determining the risk appetite, the obliged entity takes into account, *inter alia*, the relevant EBA Guidelines.
- 3.3.8. In defining risk in relation to the characteristics of persons with whom it is advisable to avoid business relationships (point 3.3.6.1 of the Guidelines), the obliged entity should not, also in the light of the objectives set out in point 3.1.8 of the Guidelines⁴⁰, exclude entire categories of customers with whom business relationships are refused by default or terminated due to the risk of money laundering and/or terrorist financing. However, such characteristics should not be defined in a way that refers to a person's general group membership⁴¹ but rather to the high-risk criteria described, for example, as activities or behavioural patterns. Within the scope of the determination of the risk appetite in relation to the characteristics that are present in persons with whom the obliged entity wants to avoid business relationships, the obliged entity will consider the various options and measures for mitigating the risks of money laundering and terrorist financing in advance, including in respect of the financial products or services it provides. The obliged entity assesses the suitability of the respective restrictions and the possibility and necessity of their implementation, considering its own risk appetite among other things.
- 3.3.9. 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, including the risks (measured) at the qualitative and quantitative levels and the compensation mechanisms, must reflect the circumstances associated with the entire group⁴². And vice versa, if an obliged entity is part of a group as a subsidiary, the risk appetite document must also take into account the relevant documents of the group, if any.
- 3.3.10. The risk appetite 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**⁴³

- 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. Also to 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, among other things:
 - 3.4.2.1. takes into account the provisions of point 3.3 of the 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 changes in risks within a reasonable time. The management board of the obliged entity or the responsible person(s) appointed at the level of the management board immediately implement measures upon the emergence of a deviation, change the organisational approach accordingly and, if necessary, suspend the provision of services in full or in part until the organisational approach has been changed.
- 3.4.3. The management board of the obliged entity must establish and regularly review the principles and

⁴⁰ See also, *inter alia*, the EBA Guidelines on policies and controls for the effective management of AML risks when providing access to financial services specified in footnote 26 and the advisory guideline of the FSA 'Requirements for providers of basic payment services' with its explanations.

⁴¹ Such as a refugee, asylum seeker.

⁴² A group within the meaning of this point is restricted only to companies that provide financial services.

⁴³ In a situation where the obliged entity has no management board, the term 'management board' is to be read as 'director of the branch' in the context of these Guidelines.

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, among other things:

- 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 be up to date with new money laundering and new terrorist financing trends, updated legislation, international practice, the FSA guidelines and other documents;
- 3.4.3.2. reviews the activity report of the AML/CFT compliance officer⁴⁴ at least once a year;
- 3.4.3.3. establishes rules of procedure for compliance with the MLTFPA and the legislative acts related thereto and the principles specified in these Guidelines (hereinafter also internal procedures) and guarantees that the employees directly involved in compliance with the MLTFPA and these Guidelines are fully aware of the requirements of the MLTFPA and these Guidelines;
- 3.4.3.4. establishes an organisational approach (including 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 approach 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 approach and include adequate human resources that comply with the risks taken at all times. In such a case the management board of the obliged entity will also create an approach that assesses the scale of the associated risks after short intervals of time and assesses the adequacy of the organisational approach for the risks taken. 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 approach;
- 3.4.3.5. ensures that the functional separation of different lines of defence and management of conflicts of interest are guaranteed. This obligation calls for, among others, regular⁴⁵ assessment of whether the bases for remuneration of managers and employees, including economic interests in respect of third parties⁴⁶, will motivate them to waive or make concessions in compliance with legislation and the Guidelines.⁴⁷ The management board guarantees an approach for identification, assessment, management and reduction of compliance or non-compliance with the aforementioned principles;
- 3.4.3.6. guarantees that the person(s) appointed by them complies (comply) with due diligence

⁴⁴ In English: *AML/CFT compliance officer*. More information on the activities of the AML/CFT compliance officer can be found in point 3.7.3.5 of the Guidelines.

⁴⁵ Regular means at least once a year.

⁴⁶ 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.

⁴⁷ See also EBA 'Guidelines on internal management' of 02.07.2021, issued as guidelines of the FSA on the basis of FSA Management Board Resolution No. 1.1-7/195 pf 15.11.2021, Divisions 11 and 12, which in the context of these Guidelines are relevant to all obliged entities. Online: https://www.fi.ee/sites/default/files/2021-11/pp%20nr%2007%20GL%20on%20internal%20governance%20under%20CRD_ET.pdf. (21.07.2023)

measures according to legislation and the recommendations made in these Guidelines and makes (make) 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 possible money laundering or terrorist financing risks;

- 3.4.3.7. ensures adequate, timely and sufficiently detailed reporting on the prevention of money laundering and terrorist financing to the competent supervisory authority.
- 3.4.4. The management board of the obliged entity must organise the effective functioning of the internal control system and ensure that the activities of the obliged entity, their managers and employees comply with legislation and the documents approved by the managing bodies as well as good practices. The management board thereby regularly assesses the efficiency of the internal procedures implemented for compliance with the MLTFPA and the Guidelines and ensures internal control of such compliance.
- 3.4.5. The management board of the obliged entity ensures that minutes are taken of the decision-making process by which it complies with the measures implemented for the performance of the obligations specified in this sub-chapter (point 3.4 of the Guidelines) and any other measures implemented for the prevention of money laundering and terrorist financing.

3.5. **Appointment of management board member in charge, their functions and role**

- 3.5.1. The obliged entity appoints the person(s) who is (are) in charge of the fulfilment of the obligations stipulated in the MLTFPA and required in these Guidelines at the level of the management board⁴⁸. Whereby:
 - 3.5.1.1. the competency and responsibility of said person must be transparently and unambiguously written down in the internal document (such as the job descriptions of members of the management board, service agreements, etc.) that regulate the duties of members of the management board;
 - 3.5.1.2. only a person who has the up-to-date and 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 management board member in charge. The management board member in charge is constantly aware of the risks that affect the obliged entity and the organisational approach that is capable of mitigating specific risks. The management board member in charge 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;
 - 3.5.1.3. the management board member in charge must devote sufficient time and resources to effectively carry out their duties in relation to the prevention of money laundering and terrorist financing. They must report on the performance of the obligations listed in point 3.5.3. and, where necessary and without delay, regularly inform the supervisory board of the obliged entity⁴⁹.
- 3.5.2. When appointing the management board member in charge, potential conflicts of interest must be identified, taken into account and, if necessary, appropriate measures implemented to avoid or

⁴⁸ If the obliged entity has more than one member of the management board, the obliged entity appoints the member of the management board who is in charge of the prevention of money laundering and terrorist financing. The director of the branch is meant in the context of these Guidelines in the case of branches.

⁴⁹ If there is a supervisory board.

mitigate them.

3.5.3. The management board member in charge must ensure that the whole management board is aware of the impact of money laundering and terrorist financing risks on the overall business. The obligations of the management board member in charge include at least the following:

3.5.3.1. to ensure that AML/CFT policies, procedures and internal control measures are adequate and proportionate considering the nature, scale and complexity of the services provided by the obliged entity and the money laundering and terrorist financing risks to which it is exposed;

3.5.3.2. to assess, with the management board, whether appointing a separate AML/CFT compliance officer⁵⁰ would be appropriate;

3.5.3.3. to assess, together with the management board, the need for a separate AML/CFT compliance unit to assist the AML/CFT compliance officer in the performance of their duties;

3.5.3.4. to ensure that reports on the activities of the AML/CFT compliance officer are regularly submitted to the management board. Also that the management board is given sufficiently detailed and timely information and data on money laundering and terrorist financing risks and compliance with the requirements of the prevention of money laundering and terrorist financing. This also includes cooperation with the competent supervisory authority, including exchange of information with the FIU;

3.5.3.5. to inform the management board of any serious or significant problems or breaches related to the prevention of money laundering and terrorist financing and to recommend appropriate measures to eliminate them;

3.5.3.6. to ensure that the AML/CFT compliance officer has: (i) direct access to all information necessary to perform their duties, (ii) adequate human and technical resources and means, and (iii) adequate information on money laundering and terrorist financing incidents and deficiencies, including those identified by internal control systems and national supervisory authorities or foreign supervisory authorities⁵¹.

3.5.4. The management board member in charge is the main contact point of the management board for the AML/CFT compliance officer. The management board must ensure that the problems raised by the AML/CFT compliance officer are addressed and taken into account as required. If the management board decides not to follow the recommendation made by the AML/CFT compliance officer, the respective decisions must be appropriately justified and documented. In the case of a significant incident, it must be possible for the AML/CFT compliance officer to go directly to the managing bodies of the obliged entity, including the supervisory board⁵².

3.6. **Activities of the Supervisory Board**⁵³

3.6.1. The supervisory board of the obliged entity is responsible for monitoring and supervising the implementation of the internal governance and control framework in order to ensure compliance with the applicable requirements in the context of the prevention of money laundering and terrorist financing. In addition to the EBA Guidelines on internal governance⁵⁴, the supervisory board must:

⁵⁰ More information on the appointment, functions and role of the AML/CFT compliance officer can be found in points 3.7.3.5.-3.7.3.8. of the Guidelines.

⁵¹ In the case of groups, by foreign authorities.

⁵² If there is a supervisory board.

⁵³ If there is a supervisory board.

⁵⁴ For the referred EBA Guidelines on internal governance, which are relevant to the activities of the supervisory board in the

- 3.6.1.1. be informed of the results of the money laundering and terrorist financing risk assessment that covers all of the operations;
 - 3.6.1.2. verify and monitor the adequacy and effectiveness of AML/CFT policies and procedures, taking into account the money laundering and terrorist financing risks of the obliged entity, and implement appropriate measures to ensure compensation mechanisms to mitigate those risks.
 - 3.6.1.3. review the activity report prepared by the AML/CFT compliance officer at least once a year. Receive updated information more frequently on activities that pose a higher risk of money laundering and terrorist financing for the obliged entity;
 - 3.6.1.4. assess, at least once a year, the effective functioning of the AML/CFT compliance function, taking into account, *inter alia*, the findings of internal and/or external audits related to the prevention of money laundering and terrorist financing. Also assess the appropriateness of the human and technical resources allocated to the AML/CFT compliance office;
- 3.6.2. The supervisory board must ensure that the AML/CFT compliance officer: (i) has the knowledge, skills and experience necessary for the identification, assessment and management of the money laundering and terrorist financing risks associated with the obliged entity and for the implementation of the AML/CFT policy, controls and procedures;(ii) has a good understanding of the business model and sector of the obliged entity and its exposure to money laundering and terrorist financing risks;(iii) receives timely information on decisions that may affect the risks of the obliged entity.
- 3.6.3. The supervisory board must have access to sufficiently detailed and quality data and information and it must take these into account in order to efficiently perform the function of money laundering and terrorist financing prevention. The supervisory board must also have timely and direct access to the activity report and reviews of the AML/CFT compliance officer, the report of the internal audit function, the conclusions and findings of external auditors. Also to the conclusions of the competent supervision authority, information exchange with the Financial Intelligence Unit and supervision measures or established enforcement measures.

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

3.7.1. General principles

- 3.7.1.1. The organisational structure of the obliged entity for the purposes of the risk management model must correspond to their size and the nature, scope and level of complexity of the activities and services provided, including the risk appetite and the associated risks, and must be built by the three lines of defence principle⁵⁵. The organisational structure of the obliged entity must correspond to the full understanding of risks and their management. Risk management is comprehensive and covers all of the activities of the obliged entity.
- 3.7.1.2. The principles of separation of functions and prevention of conflicts of interests must be taken into account in the development of the risk management model. In order to identify and manage conflicts of interests, the obliged entity:

- i. establishes a procedure for the management and prevention of conflicts of interest,

context of these Guidelines for all obliged entities, see footnote No. 47.

⁵⁵ Deviation from the principle of three lines of defence may occur where permitted by legislation, these Guidelines or other relevant guidelines (e.g. the existence of certain functions is not required and a proportionality assessment is permitted) and if the obliged entity thereby ensures the separation of functions in the organisation, i.e. adequate separation of duties upon risk taking and risk assessment, and mitigation of conflicts of interest, taking into account, among other things, the nature, scope and level of complexity of the obliged entity's activities.

which stipulates legal, technical and organisational measures, thereby considering the nature, scope and level of complexity of the activities of and services provided by the obliged entity, including the risk appetite and risks arising from activities of the obliged entity. This covers the principles of remuneration of employees (including persons in authorisation or other legal relationships) and managers;

- ii. avoids situations in the case of which the personal (including economic) interests of owners, managers and employees (including persons in authorisation or other legal relationships) and customers are in conflict with the interests of the obliged entity. This includes, above all, the interest in complying with the money laundering and terrorist financing prevention requirements arising from legislation and guidelines (including these Guidelines);
 - iii. asks their employees⁵⁶ (including persons in authorisation or other legal relationships⁵⁷) and managers⁵⁸ 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 (agents, distributors, etc.) have interests in respect of the customers⁵⁹. In the case of such a conflict of interests, the management of which must be presumed from the obliged entity, the obliged entity implements measures to manage the conflict of interests, which in some cases lies in avoiding it. In any case, the obliged entity must be ready to justify the measures implemented to the FSA and explain the content and scale of the conflict of interests. In the case of outsourcing of activities or reliance on data collected by another person, point 4.8.1 or 4.8.2 of the Guidelines will also apply.
- 3.7.1.3. 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, including the risk appetite and associated risks.
- 3.7.1.4. 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. The organisational structure and the tasks of each unit must be clearly documented.
- 3.7.1.5. Reporting and subordination chains must be guaranteed in such a manner that all employees know their place in the organisational structure and their duties.
- 3.7.1.6. The employees of the obliged entity must act with the foresight and competence expected from them and according to the requirements set for their positions. Thereby keeping in mind the interests and objectives of the obliged entity and that the economic space of Estonia is not used for money laundering and terrorist financing. The obliged entity must have established

⁵⁶ Such employees are, among others, persons who come into 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.

⁵⁷ Irrespective of the customer's risk level.

⁵⁸ *Ibid.*

⁵⁹ For example, providing them with legal services, accountancy services, services for setting up companies and other legal structures, etc.

procedures for the assessment of the suitability of employees before the commencement of their employment.

- 3.7.1.7. If the risk management function is outsourced, the principles specified in point 4.8.1. of the Guidelines apply with the relevant variations, and the provisions established in the EBA Guidelines on outsourcing⁶⁰, the advisory guideline of the FSA 'Requirements for outsourcing by subjects of financial supervision'⁶¹ and § 24 of the MLTFPA must be followed.

3.7.2. First line of defence

- 3.7.2.1. The first line of defence is a part of the risk management system related to the structural units with whose activities risks are associated and that must identify and assess these risks, their specific features and scope and that manage these risks by way of their ordinary activities, primarily by way of application of due diligence measures. The risks arising from the activities of and provision of services by the obliged entity belong to the first line of defence; they are the managers (owners) of these risks and responsible for them. This means that the application of due diligence measures upon the establishment of customer relationships (within the meaning of point 4.3 of the Guidelines) and the ordinary monitoring of customer relationships (within the meaning of point 4.4 of the Guidelines) is a function of the first line of defence.
- 3.7.2.2. The first line of defence must have good knowledge of the customer and the specific features of their activities and business activities. The employees in the first line of defence must be aware of or make themselves aware of the different specific features of the business activities of customers and the risks associated with them⁶² 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 correspond to unreasonable economic objectives or transactions that refer to such circumstances, so they can be referred to the person performing the risk management function for further analysis⁶³.
- 3.7.2.3. The management board of the obliged entity assesses, when structuring the organisational approach, 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 constant and enhanced attention). The principle highlighted in points 3.7.2.1, 3.7.2.2 and other points of the 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.
- 3.7.2.4. The duty of the first line of defence is, in the case of suspicion, to refer the identified risks, including so-called red flags in the form of suspicious and unusual transactions, to the person performing the risk management function and, if necessary, directly to the management board of the obliged entity. In line with the principle of separation of functions, it must be ensured

⁶⁰ EBA 'Guidelines on outsourcing arrangements' of 25.02.2019, issues as advisory guidelines of the FSA on the basis of FSA Management Board Resolution No. 1.1-7/92 of 05.08.2019. Online: https://www.fi.ee/sites/default/files/2019-08/pp%20nr%2004%20EBA%20Tegevuse%20edasiandmise%20suunised%20ET_0.pdf. (21.07.2023). The respective EBA Guidelines apply to credit institutions, payment institutions and e-money institutions.

⁶¹ Applies to all obliged entities except credit institutions, investment firms, payment institutions and e-money institutions. Online: <https://www.fi.ee/et/juhendid/pangandus-ja-krediit/nouded-finantsjarelevalve-subjekti-poolt-tegevuse-edasiandmisele-outsourcing-uus-redaktsioon>. (21.07.2023)

⁶² Customers, services and products, sales channels and geographic risks.

⁶³ The person performing the risk management function usually acts as a part of the second line of defence (see point 3.7.3 of the Guidelines) ensuring that all risks are identified, assessed, measured, monitored and managed. If the obliged entity has appointed a separate AML/CFT compliance officer, the person performing the risk management function may act as part of the first line of defence on the condition that the compliance with the principle of the separation of functions is ensured. The AML/CFT compliance officer should act in the second line of defence (point 3.7.3.5 (iv) of the Guidelines).

that the employees of the first line of defence who identified suspicious and unusual transactions or circumstances do not deal with the extraordinary management of risks, i.e. primarily with the analysis of suspicious and unusual transactions (excluding the identification and assessment of primary circumstances). An employee of the first line of defence passes any suspicious or unusual circumstances and transactions, including those that refer to unreasonable economic activities, on to the separately appointed and independent person performing the risk management function for further action, including for making decisions related to the performance of the reporting obligation and for risk management⁶⁴.

3.7.3. Second line of defence, including the function of the compliance officer

- 3.7.3.1. 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, including the risk appetite and risks arising from activities of the obliged entity.
- 3.7.3.2. 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.
- 3.7.3.3. 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 and to help the first line of defence manage these risks efficiently. The second line of defence does not engage in taking risks.
- 3.7.3.4. Risk policy is implemented and the risk management framework is controlled with 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 person performing the risk management function for the purposes of money laundering and terrorist financing prevention primarily performs the duties specified in points 3.3.6.3 (adherence to risk appetite and control of risk tolerance), 3.2.9 (identification of changes in risks), 3.4.3.1 (overview of associated risks), etc. of these Guidelines.
- 3.7.3.5. Where appropriate in view of the scope and level of complexity of the obliged entity's activities and the risks related to money laundering and terrorist financing, the obliged entity must appoint an AML/CFT compliance officer⁶⁵ in accordance with the EBA guidelines on AML/CFT Compliance Officers⁶⁶. Whereby:
 - i. the AML/CFT compliance officer must have sufficient authority to submit, on their own initiative, to the management board and the supervisory board⁶⁷ proposals on ensuring compliance with and the efficiency of the internal rules of money laundering and terrorist

⁶⁴ This does not mean that the employees of the first line of defence who have identified a suspicion may not act in accordance with their function as described in points 3.7.2.1 and 3.7.2.2 of these Guidelines by applying enhanced due diligence measures and the Know Your Customer principle, assisting and supporting the independent risk management function as necessary, within the scope of their (i.e. first line of defence) function.

⁶⁵ In English: *AML/CFT compliance officer*.

⁶⁶ EBA Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849 of 14.06.2022, issued as advisory guidelines of the FSA on the basis of Resolution No. 1.1-7/182 of the management board of the FSA of 21.11.2022. Online: <https://www.fi.ee/et/juhendid/pangandus-ja-krediit/euroopa-pangandusjarelevalve-suuniste-suunised-direktiivi-el-2015849-artikli-8-ja-vi-peatuki-kohase>. (21.07.2023)

⁶⁷ If there is a supervisory board.

- financing prevention;
- ii. the management board must determine whether the role of the AML/CFT compliance officer will be filled as a full-time job or in addition to other tasks. If the tasks of the AML/CFT compliance officer are assigned to an employee who also performs other tasks or functions, the management board must identify possible conflicts of interest and implement the necessary measures to prevent or manage them. The management board ensures that the employee can devote sufficient time to the performance of the duties of the AML/CFT compliance officer;
 - iii. AML/CFT compliance officer must be available to the Financial Intelligence Unit and the competent supervisory authority and, therefore, must normally also work in the country where the obliged entity is established. The obliged entity, taking into account the risks of money laundering and terrorist financing involved, may employ the AML/CFT compliance officer in another country provided that the obliged entity has the necessary systems and controls to ensure that the AML/CFT compliance officer has access to the information and systems necessary to perform the tasks and is prepared to meet with the local Financial Intelligence Unit and the competent supervisory authority without delay. The obliged entity must be able to prove to the competent supervisory authority that the established measures are adequate and efficient;
 - iv. the AML/CFT compliance officer should be part of the second line of defence and therefore part of an independent function. The following conditions must be thereby met:
 - the AML/CFT compliance officer is independent from the business lines or units they inspect and they may not be subordinate to the person who is responsible for the management of any such business line or unit;
 - the internal rules give the AML/CFT compliance officer unrestricted and direct access to all of the information they need for the performance of their tasks. The AML/CFT compliance officer thereby decides independently what kind of information they need for the performance of the tasks;
 - in the case of a significant incident, it must be possible for the AML/CFT compliance officer to go directly to the managing bodies of the obliged entity, including the supervisory board;
 - the role and tasks of the AML/CFT compliance officer are clearly defined and documented;
 - v. the AML/CFT compliance officer must have the following for the performance of their tasks:
 - an impeccable reputation, the necessary personal qualities such as honesty and integrity;
 - the relevant skills and expertise in the field of money laundering and the prevention of terrorist financing, including knowledge of the relevant legal framework and the implementation of internal procedures to prevent money laundering and terrorist financing;
 - sufficient knowledge and understanding of the money laundering and terrorist financing risks associated with the business model of the obliged entity;

- experience in identifying, assessing and managing money laundering and terrorist financing risks; and
 - sufficient time and length of service to carry out the tasks efficiently, independently and autonomously;
- vi. among other things, the AML/CFT compliance officer:
- develops and maintains the money laundering and terrorist financing risk assessment framework for money laundering and terrorist financing risks covering the whole operation of the obliged entity specified in point 3.1.6 and for individual risk assessments and maintains its compliance in accordance with the EBA Guidelines on ML/TF risk factors⁶⁸;
 - informs the management board about the results of the assessment of money laundering and terrorist financing risks. If necessary, makes proposals to the management board about risk mitigation measures;
 - ensures the establishment, updating and efficient implementation of internal procedures that are appropriate and correspond to the identified money laundering and terrorist financing risks of the obliged entity;
 - advises senior management before deciding on the establishment or continuation of a business relationship with new high-risk customers in accordance with the internal procedures of the obliged entity and in particular in situations where senior management approval is required. If senior management decides not to follow the advice of the AML/CFT compliance officer, the decision must be duly documented, including a justification of how it is intended to mitigate the risks raised;
 - verifies that the measures and internal procedures implemented by the obliged entity comply with the obligations of the obliged entity to prevent money laundering and terrorist financing. Monitors the efficient application of money laundering and terrorist financing controls of the business lines and units (first line of defence);
 - ensures that the money laundering and terrorist financing prevention framework is updated when necessary and in any case in a situation where deficiencies are found or new money laundering and terrorist financing risks become evident or changes take place in the legal framework;
 - makes proposals to the management board for elimination of the deficiencies identified in the money laundering and terrorist financing prevention framework, including for elimination of the deficiencies identified by competent supervisory authorities or by internal or external auditors;
 - advises the management board on the measures that need to be implemented in order to comply with legislation, regulations, requirements and standards, and gives estimates of the possible impact of changes in the legal or regulative framework on the activities and compliance framework of the obliged entity;
 - draws the attention of the management board member in charge of the prevention of money laundering and terrorist financing to the areas where money laundering and terrorist financing prevention controls must be implemented or improved. Gives

⁶⁸ See footnote 36.

information on the level of exposure to the risks of money laundering and terrorist financing and the measures implemented or recommended to reduce these risks and manage them efficiently. Also draws attention to whether the human and technical resources allocated to the compliance function are adequate or should be enhanced;

- prepares and submits to the management board at least once a year an activity report⁶⁹, which must be proportionate to the scope and type of the obliged entity's operations;
- informs the employees about the money laundering and terrorist financing risks they face, including the methods, trends and typologies of money laundering and terrorist financing, and the measures implemented to mitigate these risks upon a risk-based approach;
- monitors the preparation and implementation of the money laundering and terrorist financing prevention training plan. In cooperation with the relevant employee or unit, documents the annual staff training plan and covers it in the activity report to be submitted to the management board;
- assesses the training needs of the obliged entity and ensures that there is sufficient training in money laundering and terrorist financing prevention for employees. Thereby determines the assessed indicators to check the efficiency of the training;
- ensures that if the obliged entity applies a training or awareness raising plan developed in a foreign country (e.g. registered office or parent company), the plan is adapted to effective national law, including considering the obliged entity's money laundering and terrorist financing typologies and specific activities;
- ensures that, where training activities are outsourced from a service provider, (i) the service provider has the required knowledge of the prevention of money laundering and terrorist financing, (ii) conditions are imposed on the training service provider and are complied with, and (iii) the content of the training is tailored to the obliged entity;
- performs the tasks of the contact person of the FIU in the relevant case⁷⁰.

3.7.3.6. The obliged entity does not have to appoint a separate AML/CFT compliance officer if it has a very limited number of employees or if the non-appointment is justified. If the management board decides not to appoint a separate AML/CFT compliance officer, the decision must be justified and documented. The decision must be explicitly linked to at least the following criteria:

- i. the nature of the obliged entity's business operations and the related money laundering and terrorist financing risks, considering the geographic, customer, product, service and marketing channel risks;

⁶⁹ For information to be included in the activity report, see: EBA Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849 of 14.06.2022, issued as advisory guidelines of the FSA on the basis of Resolution No. 1.1-7/182 of the management board of the FSA of 21.11.2022 (point 50). Online: <https://www.fi.ee/et/juhendid/pangandus-ja-krediit/euroopa-pangandusjarelevalve-suuniste-suunised-direktiivi-el-2015849-artikli-8-ja-vi-peatuki-kohase>. (21.07.2023)

⁷⁰ Depending on the scope and level of complexity of the obliged entity's activities and the risks related to money laundering and terrorist financing, the obliged entity may decide that the tasks of the contact person of the FIU and the AML/CFT compliance officer are performed by the same person on the condition that the requirements listed in § 17 of the MLTFPA and point 3.7.3.10 are met.

- ii. the volume of the obliged entity's operations, the number of customers, the number and volume of transactions and the number of employees in FTEs⁷¹;
 - iii. the legal form of the obliged entity, including whether the obliged entity is part of a group.
- 3.7.3.7. If a separate AML/CFT compliance officer is not appointed, the obliged entity must organise the performance of the tasks of the AML/CFT compliance officer by the member of the management board specified in point 3.5 or the manager of a foreign commercial undertaking entered in the Estonian Business Register or in the outsourcing procedure⁷² or by combining said options.
- 3.7.3.8. When outsourcing the tasks of the AML/CFT compliance officer, the obliged entity proceeds from the EBA Guidelines on outsourcing⁷³, the advisory guideline of the FSA 'Requirements for outsourcing by subjects of financial supervision' as well as the main terms specified in the EBA Guidelines on outsourcing⁷⁴.
- 3.7.3.9. If the AML/CFT compliance officer works for at least two units in a group or is assigned other tasks, the obliged entity must ensure that the AML/CFT compliance officer can perform their tasks in addition to these. The AML/CFT compliance officer may act in different units only if they belong to the same group.
- 3.7.3.10. The obliged entity appoints the contact person of the FIU, who ordinarily⁷⁵ acts as part of the second line of defence. Whereby:
- i. the functions of the compliance officer may be performed by one or several employees of the obliged entity and/or a structural unit with the relevant functions. If the functions of 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 works permanently in Estonia and who has the education, professional suitability, abilities, personal qualities and experience required for performance of the duties of a compliance officer and an impeccable professional and business reputation may be appointed as a compliance officer by the management board of the obliged entity. The necessary abilities, skills and experience are assessed on the basis of the person's function and role in the structure. For example, the 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 required to understand complicated, high-value and unusual transactions that do not

⁷¹ In English full time equivalent (FTE).

⁷² Excluding the tasks of the contact person of the FIU, which cannot be outsourced pursuant to subsection 17 (4) of the MLTFPA.

⁷³ EBA 'Guidelines on outsourcing arrangements of subjects of financial supervision' of 25.02.2019, issued as advisory guidelines of the FSA on the basis of FSA Management Board Resolution No. 1.1-7/92 of 05.08.2019. Online: https://www.fi.ee/sites/default/files/2019-08/pp%20nr%2004%20EBA%20Tegevuse%20edasiandmise%20suuniste%20ET_0.pdf. (21.07.2023)

⁷⁴ EBA 'Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849' of 14.06.2022 issued as advisory guidelines of the FSA on the basis of Resolution No. 1.1-7/182 of the management board of the FSA of 21.11.2022 (points 68–73). Online: <https://www.fi.ee/et/juhendid/pangandus-ja-krediit/euroopa-pangandusjarelevalve-suuniste-suuniste-direktiivi-el-2015849-artikli-8-ja-vi-peatuki-kohase>. (21.07.2023)

⁷⁵ If the obliged entity has appointed a separate AML/CFT compliance officer, the contact person of the FIU may act as part of the first line of defence on the condition that independence from business processes and subordination to the management board member in charge or branch manager specified in point 3.5 of this Guideline is ensured.

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 independent from business processes⁷⁶;
- 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, including the information, data or documents that reflect the customer and their economic activities. The management board 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 tasks;
- 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 to terrorist financing, which have become evident in the activities of the obliged entity. For this purpose, retains all reports received from employees about suspicious and unusual transactions. Also the information and other related documents collected to analyse these reports;
 - reports to the FIU in the event of suspicion of money laundering or terrorist financing. This includes the obligation to retain the reports sent to the FIU in a format that can be reproduced in writing⁷⁷ with the time when the report was sent and the details of the employee who sent the report;
 - prepares regular 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 function of the compliance officer, or a part of the general overview of the second line of defence or of the activity report of the AML/CFT compliance officer with the compliance (and risk management) function, complying separately or with other functions with the requirements and regularity specified in point 3.7.3.12 of the Guidelines;
 - performs any other obligations directly related to the prevention of money laundering and terrorist financing;
- 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 the FSA and the Financial Intelligence Unit. The obliged entity informs the FSA within a reasonable time about the appointment of a new compliance officer or any changes in their contact details.

⁷⁶ 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.

⁷⁷ I.e. allows for it to be reproduced later.

- 3.7.3.11. If a separate contact person of the FIU is not appointed, the obliged entity must organise the performance of the tasks of the compliance officer by the member of the management board specified in point 3.5 or the manager of a foreign commercial undertaking entered in the Estonian Business Register.
- 3.7.3.12. 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 management 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, including the risk appetite and risks arising from activities of the obliged entity, but at least once a quarter, including 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, including impact on the obliged entity (both the impact of risks and the need to manage these risks via the organisational approach);
 - 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, including their impact on the obliged entity (both the impact of risks and the need to mitigate these risks via the organisational approach);
 - 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 the 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 (including internal reports and reports sent to the Financial Intelligence Unit). The analysis done on the basis of the statistics and placing this in the context of the risks associated with the activities of and services provided by the obliged entity;
 - vii. estimates of the adequacy of the compensation mechanisms of the obliged entity (including IT systems and human resources);
 - viii. proposals for amendment or updating of the obliged entity's measures 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 the occurrence of certain risks or incidents, they must be reported and overviews must also be made extraordinarily and in the *ad hoc* version. The second line of

defence decides in each case on the need to prepare an extraordinary report and on the related circumstances.

- 3.7.3.13. 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 the FSA if they identify significant omissions in the measures and actions for the prevention of money laundering and terrorist financing.

3.7.4. Third line of defence

- 3.7.4.1. The independent and effective internal audit function comprises the third line of defence of the obliged entity⁷⁸. The internal audit function may be performed by one or several employees and/or a structural unit with the relevant functions⁷⁹. The structural unit as a whole must comply with the requirements set out below. The head of the structural unit is responsible for the performance of the tasks. The main task of the internal auditor is to monitor and evaluate the operation of critical processes and systems. The person performing the internal audit function (the internal auditor) cannot assess (audit) the performance of the function they are performing (risk of self-review, conflict of interest). The same principle applies to the development of internal rules, in which the person performing the internal audit function cannot participate as they must subsequently assess the functioning of the internal control system, of which the various internal rules are an integral part.
- 3.7.4.2. The internal audit function must not be combined with the compliance function or the prevention of money laundering and terrorist financing.
- 3.7.4.3. 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 person performing 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, including the risk appetite and risks arising from activities of the obliged entity.
- 3.7.4.4. The person performing the internal audit function or the head of the structural unit performing the internal audit 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 performing 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.
- 3.7.4.5. The internal audit function assesses, among others, whether:
- i. the management framework of the obliged entity is suitable for the prevention of money laundering and terrorist financing;
 - 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. activities/procedures are in compliance with the applicable legislation and rules of

⁷⁸ 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 3.7.4 of these Guidelines.

⁷⁹ The internal audit function may be outsourced to a third party.

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, which 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 holistic⁸⁰ view) are appropriate and adequate for the prevention of money laundering and terrorist financing, correspond to the organisation's needs and the expectations of supervisory authorities.

3.7.4.6. 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, including 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 in its work from the risk-based and proportionality principle.

3.7.4.7. If the internal audit function is outsourced, the obliged entity ensures compliance with, among others, the requirements arising from the Guidelines, primarily from point 3.7.4.5 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) regularly assesses whether outsourcing the internal audit function is justified and the efficiency of the internal audit.

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

3.8. Business continuity and events of operational and reputational risk

3.8.1. 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.

3.8.2. The measures implemented must at least cover the activities required to ensure the business continuity of compensation mechanisms. Also the activities required in the situations where the business continuity of compensation mechanisms is discontinued.

3.8.3. The obliged entity also informs the FSA as soon as possible about the significant incidents related to the business continuity of the significant compensation mechanisms and other significant operational and reputation risks incidents related to the prevention of money laundering and terrorist financing and the measures implemented.

3.9. Training

3.9.1. 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, including 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

⁸⁰ In English – holistic view.

defence.

- 3.9.2. Above all, the persons covered by the training must be aware of the requirements of money laundering and terrorist financing prevention in regard to the application of due diligence measures and reporting suspicions of money laundering. The training must give information about, among others, the following:
 - 3.9.2.1. the principles specified in the risk appetite document of the obliged entity⁸¹;
 - 3.9.2.2. the risks arising from the activities of and services provided by the obliged entity⁸², including risks foreseen in the future;
 - 3.9.2.3. the obligations to prevent money laundering and terrorist financing set forth in the rules of procedure and compliance with them;
 - 3.9.2.4. the contemporary methods of committing money laundering and terrorist financing and specific typologies/cases, and the risks associated with them;
 - 3.9.2.5. how to recognise actions related to possible money laundering or terrorist financing, and guidelines on how to act in such situations.
 - 3.9.3. The content of the training for employees exposed to different levels of money laundering and terrorist financing risks must be tailored to the risk.
 - 3.9.4. 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. The obliged entity must ensure that training is tailored to the employees and their specific roles.
 - 3.9.5. 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, including the risk appetite and risks arising from activities of the obliged entity, but it usually takes place at least once a year. If necessary, training is organised or employees are informed more frequently, including 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 become evident, etc.
 - 3.9.6. 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.
- 3.10. Establishment of and requirements for rules of procedure**
- 3.10.1. The obliged entity establishes and implements rules of procedure for the efficient mitigation and management of risks related to money laundering and terrorist financing. The complexity and structure of the rules of procedure must comply with the size of the obliged entity and the nature, scope and level of complexity of the activities and services, including the risk appetite and risks arising from activities of the obliged entity.
 - 3.10.2. The rules of procedure include at least the following:
 - 3.10.2.1. the procedure for assessment of the risks related to the obliged entity's operations. Also

⁸¹ Considering the document prepared on the basis of point 3.2 of these Guidelines.

⁸² Considering the document prepared on the basis of point 3.3.10 of these Guidelines.

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

- 3.10.2.2. the procedure for prevention of conflicts of interests (see also point 3.7.1.2 of the Guidelines);
- 3.10.2.3. 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 the Guidelines);
- 3.10.2.4. 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 the Guidelines, among other things, and the procedure for application of due diligence measures to customers (both the procedure for application of simplified and enhanced due diligence measures). The activities of the different lines of defence of risk management⁸³ that 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 a person subject to international sanctions or a person whose place of residence or location is in a high-risk third country or in a country that meets the conditions specified in subsection 37 (4) of the MLTFPA.
- 3.10.2.5. The tasks, rights and roles of the contact person of compliance, including the contact person of the FIU, and the person performing the risk management function, which are not covered by point 3.10.2.4 of the Guidelines. The provisions of clause 3.7.3 of the Guidelines must be taken into account in the case of tasks.
- 3.10.2.6. The procedure for collection and retention of records. Also the procedure for making them accessible.
- 3.10.2.7. The situations where the employees of the first line of defence of risk management or the other employees of the obliged entity who have become aware of the respective information must notify the contact person of the FIU about suspicions of money laundering and terrorist financing or unusual transactions or circumstances.
- 3.10.2.8. The procedure for refusal to establish a business relationship or refusal of an occasional transaction (within the meaning of point 6.1 of the Guidelines), the procedure for exercising the right to refuse to conclude a transaction (within the meaning of point 6.2 of the Guidelines) and the procedure for extraordinary cancellation of a business relationship (within the meaning of point 6.3 of the Guidelines). Also (i) who makes the relevant decisions, (ii) who implements these decisions (who closes the relevant accesses of the customer in the obliged entity's systems, makes the relevant notices in the system, informs the customer, etc. and when), (iii) how the contact person of the FIU is informed about the circumstances, and (iv) reporting to the FIU when appropriate.
- 3.10.2.9. The procedure for reporting to the FIU (within the meaning of point 7 of the Guidelines), including (i) the procedure for reporting on internally suspicious and unusual transactions or circumstances, (ii) the methodology and the guidelines from which the compliance officer proceeds when analysing suspicious and unusual transactions or circumstances, and

⁸³ 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.

(iii) the methodology and the guidelines if the obliged entity suspects money laundering or terrorist financing or an unusual transaction or circumstance is detected.

3.10.2.10. The procedure for outsourcing (see point 4.8.1 of the Guidelines) and relying on data collected by another person (see point 4.8.2 of the Guidelines).

3.10.2.11. 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, including the management board, and the persons to whom activities have been outsourced;

3.10.2.12. In the case of relationships with other credit or financing institutions, the procedure for the establishment and continuation of correspondent relationships (see point 4.9 of the Guidelines);

3.10.2.13. the procedure for the renewal of the rules of procedure;

3.10.2.14. The procedure for performance of the other obligations arising from the Guidelines.

3.10.3. 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, including the procedure for implementation of an internal audit and, where necessary, compliance, where the procedure for checking employees is described, among others.

3.10.4. 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.

3.10.5. The obliged entity regularly checks that the established rules of procedure and internal control rules are up to date, including 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.

3.10.6. The obliged entity specifies the names of 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.

3.10.7. 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.

3.11. Risk management and measures in a group

3.11.1. In the event of groups where the obliged entity is in the function of a parent company⁸⁴, 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 group⁸⁵.

⁸⁴ In English – parent company.

⁸⁵ 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 of undertakings that consists of a parent undertaking, its subsidiaries within the meaning of § 6 of the Commercial Code, and the entities in which the parent undertaking or its

- 3.11.2. 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 3.3.9 of the Guidelines).
- 3.11.3. In the case of group membership as a 'parent company', the obliged entity must ensure that it has sufficient data and information and is able to assess the group-wide money laundering and terrorist financing risk profile in line with the EBA Guidelines on risk factors⁸⁶.
- 3.11.4. In the case of a group, the group-wide rules of procedure must cover at least the following:
- 3.11.4.1. the group-wide procedure for assessment of risks and definition of risk appetite;
 - 3.11.4.2. 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;
 - 3.11.4.3. a description of the organisational approach for the prevention of money laundering in the group, which among others includes the principle of the three lines of defence (see also point 3.7 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;
 - 3.11.4.4. 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 the application of due diligence measures and the 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 FIU and the documents serving as a basis for this. The obliged entity must ensure that information on a suspicion reported to the FIU is shared within the group, unless the FIU has ordered otherwise.
 - 3.11.4.5. 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-off⁸⁷) and the restrictions on the use of information transmitted in the group;
 - 3.11.4.6. a description of the measures on the basis of which the suitability of employees is assessed before the commencement of their employment (see also point 3.7.1.6 of these Guidelines);
 - 3.11.4.7. the procedure for training the employees who are involved in the prevention of money laundering and terrorist financing as well as the senior management, including the management board, and the persons to whom activities have been outsourced.
 - 3.11.4.8. the internal control rules that cover the procedure and measures for the functioning of the independent audit function. This also covers the measures implemented to ensure that the group companies implement group-wide policies and take into account the established risk appetite in other respects.

subsidiaries hold participation as well as undertakings that constitute a consolidation group for the purposes of subsection 3 of § 27 of the Accounting Act;

⁸⁶ See footnote 36.

⁸⁷ In English – tipping-off.

- 3.11.5. 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.
- 3.11.6. 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, including the risk assessments of the law enforcement agencies or supervisory authorities of the European Union, Estonia or such other country.
- 3.11.7. 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.
- 3.11.8. The obliged entity must ensure that the due diligence measures applied in their groups located in third countries and the requirements for the collection and retention of data comply with the requirements set out in the MLTFPA and these Guidelines. The FSA 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 implemented 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. The FSA must be informed of any additional measures implemented.
- 3.11.9. 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 the FSA about this and submit the explanations and reasons for the decision made.
- 3.11.10. In the case of group membership as a 'parent company', the obliged entity must ensure that each managing body⁸⁸, business line and internal unit, including each internal control function, has the information necessary to perform its functions. In particular, it must ensure adequate communication between the business lines and the unit responsible for the compliance function concerning the prevention of money laundering and terrorist financing and, where these are different functions, between the compliance functions at group level and between the heads of the internal control functions at group level and the managing body of the obliged entity.
- 3.11.11. In the case of group membership as a 'parent company', the managing body of the parent company must perform at least the following functions:
- 3.11.11.1. in order to gain an overview of the money laundering and terrorist financing risks to which each entity within the group (hereinafter referred to as group entity) is exposed, ensure that group entities assess business-wide money laundering and terrorist financing risks in a coordinated manner and on the basis of a common methodology, taking into account the specificities of their business and the EBA Guidelines on risk factors⁸⁹;
- 3.11.11.2. ensures that all deficiencies and breaches identified in the supervisory activities of the

⁸⁸ The supervisory board or the management board.

⁸⁹ See footnote 36.

competent supervisory authority in each group entity have been remedied in a timely and effective manner and that all corrective actions have been completed in a timely and effective manner.

3.11.12. In the case of group membership as a 'parent company', the obliged entity must:

- 3.11.12.1. appoint the management board member in charge of the prevention of money laundering and terrorist financing and the AML/CFT compliance officer of the group;
- 3.11.12.2. create a structure at group level with sufficient decision-making rights for the management of money laundering and terrorist financing prevention in the group;
- 3.11.12.3. approve the intra-group policies and procedures for the prevention of money laundering and terrorist financing;
- 3.11.12.4. establish intra-group control mechanisms for the prevention of money laundering and terrorist financing;
- 3.11.12.5. regularly assess the efficiency of the policies and procedures for the prevention of money laundering and terrorist financing at group level;
- 3.11.12.6. the obliged entity that manages branches or subsidiaries nationally or in another Member State or in a third country appoints the compliance officer of the group, who ensures that all group entities implement the group's money laundering and terrorist financing prevention policy and have adequate and appropriate systems and procedures for the efficient prevention of money laundering and terrorist financing.

3.11.13. The AML/CFT compliance officer of the group must cooperate fully with the AML/CFT compliance officers of each unit of the group.

3.11.14. The AML/CFT compliance officer of the group must perform at least the following tasks:

- 3.11.14.1. coordinate the assessment of the risk of money laundering and terrorist financing that covers the operations of the entire group. The assessment is carried out by group entities at the local level. The AML/CFT compliance officer of the group must organise the aggregation of these results to understand the type, intensity and location of the money laundering and terrorist financing risks to which the group as a whole is exposed;
- 3.11.14.2. prepare a money laundering and terrorist financing risk analysis that covers the whole group;
- 3.11.14.3. define the money laundering and terrorist financing prevention standards at group level. Ensure that the group's policies and procedures at the local level comply with the legislation and requirements of money laundering and terrorist financing prevention, which are applied separately to each group unit, including in accordance with the group's standards;
- 3.11.14.4. coordinate the activities of local AML/CFT compliance officers in the group's AML/CFT units to ensure their consistent functioning;
- 3.11.14.5. monitor the compliance of branches and subsidiaries in third countries with EU rules on money laundering and terrorist financing prevention;
- 3.11.14.6. establish, in accordance with national law, group-wide policies, procedures and measures concerning, *inter alia*, the intra-group exchange of information for the purposes of preventing money laundering and terrorist financing and data protection;
- 3.11.14.7. ensure that group entities have adequate procedures in place to report suspicious transactions or activities and that group entities properly share information, including information on reporting, without violating confidentiality requirements.

3.11.15. The AML/CFT compliance officer of the group prepares an activity report⁹⁰ once a year and submits it to the management board.

3.11.16. The AML/CFT compliance officer of the subsidiary or branch must have a direct reporting line with the AML/CFT compliance officers of the group.

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 laundering⁹¹, prevent the financing of terrorism from illegal or legal sources of money, prevent the proliferation financing or evasion of sanctions, 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, proliferation financing and evasion of sanctions.

4.1.2. Due diligence measures must be applied to the extent prescribed in the MLTFPA and adequately so that the obliged entity is convinced of the mitigation of the risks of money laundering and terrorist financing. The obliged entity has applied due diligence measures adequately if the obliged entity has the inner conviction that they have complied with the obligation to apply due diligence measures. The principle of reasonability is observed in the consideration of inner conviction. This means that the obliged entity must, upon the application of due diligence measures, acquire the knowledge, understanding and 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 and, where appropriate, the wealth, etc. so that they understand the customer and customer's (business) activities, thereby taking into account the customer's risk level⁹², the risk associated with the business relationship and the nature of such relationship (i.e. the risk profile of the business relationship). Such 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). The achievement of conviction must also be visible (records must be kept) to the competent supervisory authority and the obliged entity must be able to explain the extent

⁹⁰ For information to be included in the activity report, see: EBA Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT Compliance Officer under Article 8 and Chapter VI of Directive (EU) 2015/849 of 14.06.2022, issued as advisory guidelines of the FSA on the basis of Resolution No. 1.1-7/182 of the management board of the FSA of 21.11.2022 (point 82). Online: <https://www.fi.ee/et/juhendid/pangandus-ja-krediit/euroopa-pangandusjarelevalve-suuniste-suunised-direktiivi-el-2015849-artikli-8-ja-vi-peatuki-kohase>. (21.07.2023)

⁹¹ In English – placement, layering and integration.

⁹² 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, including implement additional measures to make sure the data are correct. In this manner, the submitted data must give the obliged entity the inner conviction (including based on 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.

of the due diligence measures applied and the achievement of conviction.

4.1.3. The application of due diligence measures divides into due diligence upon the establishment of a business relationship, conclusion or mediation of occasional transactions outside 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 implemented 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, including using means of electronic identification and of trust services for electronic transactions (see points 4.3.1 and 4.3.2 of the 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 the Guidelines).
- iii. identifying the beneficial owner and application of measures for verifying their identity to the extent that makes it possible for the obliged entity to become convinced of who the beneficial owner is. Also understands the ownership and control structure of the customer or the person participating in an occasional transaction (see point 4.3.3. of the 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 the Guidelines);
- v. identification of the source and/or origin of wealth if appropriate (see point 4.3.5 of the Guidelines);
- vi. understanding of business relationships or an occasional transaction and, where relevant, gathering additional information thereon (see point 4.3.6 of the Guidelines).

4.1.4.2. The purpose of application of due diligence measures is to comply with the Know Your Customer principle⁹³. Upon compliance with said 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 comply with the customer's actual activities, capacity 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 3.2 of the 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 apply 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

⁹³ In English – Know-Your-Customer, KYC.

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 based on the information already collected. Thus, the regime of monitoring the business relationship is defined on the basis of the customer's 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 upon the application of due diligence measures are usually also specified in the customer questionnaire prepared about the customer and approved 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, including 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 the submission of false data.

4.1.5. Upon the monitoring of a business relationship

- 4.1.5.1. The due diligence measures 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 the 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 the Guidelines);
- iii. identification of the source and origin of the funds used in a transaction (see point 4.4.3 of the 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.

- 4.1.5.3. More attention must be given to:

- i. the transactions made in the business relationship, the customer's activity and circumstances that refer to criminal activity, money laundering or terrorist financing or that may be connected to money laundering or terrorist financing, including complex, high value or unusual transactions or transaction patterns, which have no reasonable or evident economic or legal objective or which is not characteristic of the specific business⁹⁴;
- ii. business relationship or transaction if the customer is from a high-risk third country or a country or territory specified in subsection 37 (4) of the MLTFPA or if the customer is a

⁹⁴ The nature, reason and background of the transactions as well as other information that allows for understanding the substance of the transactions must be identified and more attention must be paid to these transactions.

citizen of such country or if the customer's place of residence or location or the registered office of the payment service provider of the payee is in such country or territory.

4.1.6. The obliged entity must apply all due diligence measures⁹⁵, i.e. they may not leave any due diligence measures unapplied at 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 using a risk-based approach⁹⁶ and according to the principles suitable for the business strategy. Due diligence measures are applied to the extent corresponding to the 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 and during a business relationship;

4.1.7.2. in the case of money transfers⁹⁷ made as occasional transactions where the transaction value exceeds €1,000 or an equivalent sum in another currency, regardless of whether the financial obligation is performed in the transaction as a one-off payment or as several related payments over a period of one month. Due diligence measures must thereby be applied as soon as the fact that said amount is exceeded becomes known. If exceeding the amount depends on several related payments being made, then from the moment when the sum is exceeded. In the case of money transfers made as an occasional transaction, where the value of the transaction is up to €1,000, the application of due diligence measures may be limited to the identification and verification of the identity of the person involved in the transaction⁹⁸;

4.1.7.3. upon making or mediating occasional transactions outside a business relationship where the value of the transaction is at least €15,000 or an equal amount in another currency⁹⁹, 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 arrival of the aforementioned sum becomes known or, where the arrival of the sum depends on the making of several linked payments, as soon as the sum is

⁹⁵ Excluding the case stipulated in point 4.8.3 of these Guidelines.

⁹⁶ See also point 4.2 of these Guidelines.

⁹⁷ 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, 05.06.2015, pp 1–18). Online: <https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:02015R0847-20200101>. (21.07.2023)

⁹⁸ Credit and financial institutions must identify the parties to the transaction in the case of all transactions (subsection 25 (1) of the MLTFPA). In the case of money transfers made as occasional transactions the value of which exceeds €1,000, credit and financial institutions must also apply other due diligence measures in addition to identification and verification of identity (subsection 25 (1¹) of the MLTFPA). An obliged entity that is not a credit or financing institution within the meaning of § 6 of the MLTFPA, also a credit or financial institution in an appropriate case (occasional transactions that are not money transfers within the meaning of the regulation specified in footnote 95), applies due diligence measures upon the conclusion or mediation of occasional transactions outside a business relationship, considering the limit set in point 4.1.7.3 of the Guideline and clause 19 (1) 2) of the MLTFPA.

⁹⁹ The obliged entity thereby assesses the situation where a person participating in an occasionally concluded transaction knowingly or in a manner that refers to such activities concludes transactions once or several times in amounts smaller than €15,000 and takes into account that such transactions may refer to suspicious or unusual transactions, which is why the obliged entity must perform additional obligations (including refusal to conclude the transaction and the obligation to notify the FIU).

exceeded;

- 4.1.7.4. 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;
 - 4.1.7.5. upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits provided by law.
 - 4.1.8. 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 persons¹⁰⁰. Legislation requires 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 transactions or if their activities create suspicions of money laundering or terrorist financing (see also point 6.1 of the Guidelines). In certain cases, the obliged entity is obliged to exercise the right to refuse a transaction concluded within the scope of the business relationship (see also point 6.2 of the Guidelines). Legislation also stipulates the obligation of the obliged entities to cancel a long-term contract without notice if the person does not submit sufficient information for the application of due diligence measures (see point 6.3 of the Guidelines).
 - 4.1.9. Upon the application of any due diligence measure, the obliged entity takes into account the money laundering and terrorist financing risks and methods characteristic of Estonia given in Annexes 1 and 2 to the Guidelines.
 - 4.1.10. 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 transactions¹⁰¹.
 - 4.1.11. The information and data collected in the course of the application of due diligence measures and the measures implemented for the prevention of money laundering and terrorist financing must be retained (see point 5 of the Guidelines).
 - 4.1.12. The management board of the obliged entity must ensure compliance with due diligence according to the recommendations made in the 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 (including the risks that emerge before the application of compensation measures). 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, including the possible threats must be assessed, which may affect the activities of the customer or the obliged entity and

¹⁰⁰ See also footnote 95.

¹⁰¹ 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.

the possibility that the probability of the emergence of the given threat will increase.

- 4.2.2. The obliged entity acknowledges that the application of the risk-based approach, also taking into account the objectives set out in point 3.1.8 of the Guidelines and the provisions set out in point 3.3.8, does not mean that the obliged entity must refuse to establish business relationships with certain categories of customers, which it associates with a higher risk of money laundering and terrorist financing, or terminate these business relationships, insofar as the risk associated with individual business relationships may vary in the same category of customers.
- 4.2.3. 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).
- 4.2.4. Determination of the risk level means that the obliged entity considers, in the case of certain customers or business relationships, the activities or actions not expected to be possible¹⁰², which is why more attention must be given to the customer and their activities or on the contrary, or does not consider such activities possible from certain customers, which is why the extent to which attention is given is different. Determining a risk level that is higher than usual does not mean that this 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 circumstances as a set. Neither does determining a lower risk level mean that the customer cannot be associated with money laundering or terrorist financing. The obliged entity must continuously assess the risks associated with customers in order to mitigate money laundering and terrorist financing risks.
- 4.2.5. In order to determine the risk profile and risk level, the obliged entity takes into account:
 - 4.2.5.1. the risk assessment prepared on the basis of point 3.2 of the Guidelines;
 - 4.2.5.2. the purpose of the business relationship or the occasional transaction or operation, and the information that the obliged entity has collected about the objective of the business relationship or the occasional transaction or operation within the meaning of point 4.3.6 of the Guidelines, considering the factors specified in Annexes 1 and 2 to the Guidelines;
 - 4.2.5.3. the volume of the assets deposited by the customer or the value of an occasional transaction;
 - 4.2.5.4. the expected duration of the business relationship;
 - 4.2.5.5. 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;
 - 4.2.5.6. 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, the FATF and the EBA); and
 - 4.2.5.7. primarily the guidelines of the EBA¹⁰³ (including the risk factors specified therein), which

¹⁰² Considering primarily the nature, scope and level of complexity of their services, including the risk appetite and risks associated with the activities of the obliged entity.

¹⁰³ See footnote 36.

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.

4.2.6. 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:

- 4.2.6.1. 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);
- 4.2.6.2. the weight of risk factors may not be influenced by the economic or profit-related considerations of the obliged entity;
- 4.2.6.3. 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;
- 4.2.6.4. 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
- 4.2.6.5. consideration of the risk factors of the customer may not be in conflict with the relevant directives of the European Parliament and of the Council¹⁰⁴, the MLTFPA or this Guideline, which describe the situations that always refer to a higher risk/threat of money laundering or terrorist financing.

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

- 4.2.7.1. upon identification of a person or verification of submitted information, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
- 4.2.7.2. the customer or the beneficial owner is a high-risk politically exposed person (see also point 4.3.4 of the Guidelines);
- 4.2.7.3. the obliged entity establishes a correspondent relationship with a respondent institution whose risk of money laundering or terrorist financing is high or with a third country correspondent institution (see also point 4.9 of these Guidelines);
- 4.2.7.4. the obliged entity deals with or provides services to natural persons or legal entities that originate in a high-risk or non-cooperating country entered in the FATF high-risk country list¹⁰⁵, the EU list of non-cooperative jurisdictions for tax purposes, a high-risk third country¹⁰⁶ or a higher risk¹⁰⁷ country or territory or they have the citizenship of such a country or their

¹⁰⁴ 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.

¹⁰⁵ See the following relevant FATF lists: 'High-Risk Jurisdictions subject to a Call for Action' and 'Jurisdictions under Increased Monitoring'.

¹⁰⁶ High-risk third country according to Directive (EU) 2015/849 of the European Parliament and of the Council and Commission Delegated Regulation (EU) No. 2016/1675.

¹⁰⁷ The definition of high-risk countries is not always list-based. Many of the factors that increase geographic risk are not list-based, for example, corruption is generally measured by indices rather than making binary judgements about countries.

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 the Guidelines);

- 4.2.7.5. 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 the Guidelines);
- 4.2.7.6. several of the circumstances referring to the risks highlighted in the NRA or Annexes 1 and 2 to the Guidelines are present at the same time.
- 4.2.8. In order to identify the risk factors, the obliged entity applies additional due diligence measures if necessary, including 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 the Guidelines).
- 4.2.9. The obliged entity applies measures, including enhanced due diligence measures in appropriate cases, within the meaning of point 4.6 of the 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.
- 4.2.10. If the automatically assigned risk levels must be reassessed, the reasons of the reassessment must always be appropriately documented.
- 4.2.11. 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 justifying why giving additional attention to the customer or their activities is no longer necessary. When the risk level is changed in such a manner, the obliged entity must be prepared to explain (including to the FSA), 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 determination of a higher risk level does not mean that the customer may not perform such transactions or actions in the future or that the features and circumstances referring to a higher risk level have been overcome/have disappeared, etc.
- 4.2.12. 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 natural person and representative

General principles

- 4.3.1.1. Upon the establishment of a business relationship or the conclusion of an occasional transaction, the obliged entity must identify the natural person who is the customer or the

Higher risk countries and jurisdictions are, among others, those that:

- 1) according to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, have not established effective money laundering and terrorist financing prevention systems;
- 2) according to credible sources, have significant levels of corruption or other criminal activity;
- 3) are subject to sanctions, embargoes or similar measures issued by, for example, the European Union or the United Nations;
- 4) 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) the obliged entity itself defines as higher risk countries.

person participating in an occasional transaction and verify the submitted information on the basis of the information obtained from a trustworthy 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 4.3.1.29 of the 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 the 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 the 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 4.3.1.25 to 4.3.1.28 of the 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 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, including 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 the 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. The identity of the public figures and persons directly or indirectly related to them who address the obliged entity to make transactions or perform acts must also be verified.
- 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 service¹⁰⁸. 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 relationship¹⁰⁹. 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 (including the data collected upon 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 the Guidelines or that the business relationship should not be monitored within the meaning of point 4.4 of the 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

¹⁰⁸ In the case of the limits specified in point 4.3.1.14 of these Guidelines, the total amount of all such outgoing payments must be cumulatively taken into account.

¹⁰⁹ 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.

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 the FSA, including demonstrate why the source is reliable and independent and 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. The obliged entity must also be prepared to show the competent supervisory authority the activities carried out and the data collected by means of remote identification (e.g. video interview).

Time of identification

- 4.3.1.9. Identity must be always ascertained and verified within a 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 conclusion of the transaction or during the conclusion 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. For the purposes of identification, the following data (or information for the purposes of this guide) is collected and retained:

- i. the name of the person;
- ii. the person's personal identification code, or if the person doesn't have one, their date of birth and place of residence or location,
- iii. information on the identification and verification of the right of representation and scope thereof and, where the right of representation does not arise from law, the name of the document serving as the basis for the right of representation, the date of issue, and the name of the issuer;
- iv. details of the means of communication;

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

- v. place of residence¹¹⁰;
- vi. profession or area of activity, if necessary¹¹¹.

¹¹⁰ 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 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.

¹¹¹ Asking about the profession or area of activity is not an imperative obligation or something that must always be requested upon identification, but it may be important for the identification of the objective of the business relationship (in the

- 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 officially¹¹² certified or other information from a reliable and independent source, including means of e-identification and trust services of e-transactions, using at least two sources for the verification of data in such a case¹¹³.
- 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 the Guidelines are true and correct (first two sub-points)¹¹⁴, also confirming, if necessary, that the data directly related to the person (fifth and 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 to be.
- 4.3.1.14. Verification of information collected in the course of identification of a person¹¹⁵:
- i. must be carried out face-to-face or with IT tools (i.e. video identification) if (i) the customer is from a country outside the European Economic Area or their place of residence or business is in such a country, or (ii) the total amount of the outgoing payments per calendar month exceeds €15,000 in the case of a natural person and €25,000 in the case of a legal entity, irrespective of the person's origin or their place of residence or location;
 - ii. must therefore not be carried out face-to-face or with an IT tool (i.e. video identification) and the possibility stipulated in point 4.3.1.19 of the Guidelines (two

confluence of clause 20 (1) 4) and subsection 20 (2) of the MLTFPA, see also point 4.3.6 of the Guidelines), 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 (whether the person works in the position of a politically exposed person).

¹¹² 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.

¹¹³ The requirement that two sources must be used does not need to be applied to a customer with restricted active legal capacity and on whose behalf a business relationship is established or a transaction is entered into by their representative.

¹¹⁴ 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.

¹¹⁵ 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.

sources) can be used instead if (i) the total amount of the outgoing payments per calendar month is less than €15,000 in the case of a natural person and less than €25,000 in the case of a legal entity; and the person is from a Contracting State of the European Economic Area of 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 the Guidelines by comparing the person's biometrics (facial image) with the facial image on or obtained from the document¹¹⁶ specified in point 4.3.1.11 of the 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 and verification of data with IT tools, 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 Finance¹¹⁷ 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 document¹¹⁸ specified in point 4.3.1.11 of the Guidelines.
- 4.3.1.17. In situations where the obliged entity does not carry out the identification and data verification in the same place, i.e. face-to-face, the obliged entity must further comply with the EBA Guidelines on remote customer onboarding¹¹⁹ when carrying out the identification and data verification. If national law provides for stricter requirements than the EBA Guidelines on remote customer onboarding, national law should be applied.

¹¹⁶ 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).

¹¹⁷ Minister of Finance regulation No. 25 of 23.05.2018 'Technical requirements and procedures for identification and verification of data by means of information technology' - RT I, 04.12.2020, 9.

¹¹⁸ 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).

¹¹⁹ EBA 22.11.2022 'Guidelines on remote customer onboarding in accordance with Article 13(1) of Directive (EU) 2015/849', issued in part FSA Management Board Resolution No. 1.1-7/97 of 29.05.2023, i.e. with the exception of points 15(a), 25(a) and 45(a) of the Guidelines and to the extent related thereto, according to which credit and financial institutions should deem the criteria set out in points 14(a), (d) and (e), 24 and 38 to 43 of the Guidelines met if the remote onboarding solution uses e-identification systems, which have been reported in accordance with Article 9 of Regulation (EU) No. 910/2014 and which meet the requirements for the 'significant' level of confidence in accordance with Article 8 of the same Regulation, where the customer is identified by means of information technology in accordance with § 31 of the MLTFPA and the Minister of Finance Regulation 'Technical Requirements and Procedures for Identification and Verification of Data by Information Technology Tools' established on the basis of subsection (6) of the same section. The Guidelines will apply to the extent set out above from 02.10.2023. Online: <https://www.fi.ee/et/juhendid/pangandus-ja-krediit/suunised-klientide-kaugtuvastamise-lahenduste-kohta-kooskolas-direktiivi-el-2015849-artikli-13>. (21.07.2023)

Reliable and independent source

- 4.3.1.18. The (i) face-to-face identification¹²⁰ or (ii) identification with IT tools¹²¹ 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 the 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.
- 4.3.1.19. In situations not specified in point 4.3.1.18 of the Guidelines, the reliable and independent source (must exist cumulatively) is verification of the information obtained in the course of identification, (a) which comes from two sources, (b) where, if the money laundering and terrorist financing risk of the customer and the business relationship is average or higher than usual, the customer sends a photo taken of the facial image of the person for the specific financial service immediately before the data are sent and the obliged entity makes sure that the photo was taken recently,¹²² and (c) which corresponds to the following features, i.e. a 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. it is neutral (e.g. information obtained from the Internet is not such information, as it often comes 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 whose 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).
- 4.3.1.20. 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 document¹²³.
- 4.3.1.21. When obtaining reliable and independent information, the obliged entity must ensure, especially in the case stipulated in point 4.3.1.19 of the Guidelines, that the obtained reliable and independent information is not a so-called black and white and/or illegible copy.
- 4.3.1.22. 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

¹²⁰ See also point 4.3.1.15 of the Guidelines.

¹²¹ See also point 4.3.1.16. of the Guidelines.

¹²² 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.

¹²³ 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 4.3.1.23 of the 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 4.3.1.23 of the Guidelines).

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

4.3.1.23. one of the sources is always:

- i. an identity document with a photo stipulated in point 4.3.1.11 of the 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 sources¹²⁴; 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, and place of residence or business) obtained in the course of strong authentication¹²⁵ carried out with a digital personal identification tool if the money laundering and terrorist financing risk associated with the client and the business relationship is lower than usual, and the audit trail proving that this was done.

4.3.1.24. 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 4.3.1.23 of the 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 of birth if there is no personal identification code and place of residence or business) obtained in the course of strong authentication¹²⁶ carried out with a digital personal identification tool and the audit trail proving that this was done¹²⁷; or
- iii. verification of the data directly related to a person via the Population Register¹²⁸ or an equivalent register, provided that the source is a reliable and independent source within the meaning of point 4.3.1.19 of the Guidelines; or
- iv. information received from a check payment¹²⁹; 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

¹²⁴ For example, a document photo obtained from the Police and Border Guard Board.

¹²⁵ 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.

¹²⁶ *Ibid.*

¹²⁷ 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 4.3.1.23 of the Guidelines. Upon the implementation of sub-point 3 of point 4.3.1.23 of these Guidelines, strong authentication can only be used with another digital identification tool that allows for strong authentication.

¹²⁸ Legal entities and natural persons may access the Population Register in the case of legitimate interest.

¹²⁹ This means that the customer or a person participating in the transaction makes a transfer to the obliged entity's account from a current 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.

work, residence or study)¹³⁰.

Differences in the case of representation

- 4.3.1.25. 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 which the basis of the right of representation must be ascertained and retained¹³¹.
- 4.3.1.26. 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)¹³², unless otherwise stipulated in the international agreement.
- 4.3.1.27. When the right of representation of authorised and legal representatives is handled, it must be ascertained whether the representative knows their customer¹³³. 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. 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 and convinced of the source and legal origin of the funds used by the represented person in the transaction.
- 4.3.1.28. 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

- 4.3.1.29. Upon the identification of a natural person, the obliged entity must also identify the beneficial owner of the natural person¹³⁴, i.e. the person who controls and benefits from the person's activity.
- 4.3.1.30. 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 implement all measures to identify the beneficial owner of the trust within the meaning of point 4.3.3 of the Guidelines and perform all actions to ascertain the actual purpose of the business relationship within the meaning of point 4.3.6 of the Guidelines. For the purposes of the General Part of the Civil Code Act, this may mean that a

¹³⁰ 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.

¹³¹ 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.

¹³² See point 4.3.2.16 of the Guidelines for legalisation and Apostille.

¹³³ A person representing a legal entity is expected to know the entity's economic and professional activity, i.e. the area of occupation or activity, the authorisation, the objectives of their transactions, payment practices, main partners, source and origin of the funds used in transactions, owners, etc.

¹³⁴ Both the so-called 5th Anti-Money Laundering Directive (see footnote 16) and FATF Recommendation 10 require the beneficial owner to be identified at all times, i.e. even when the customer or the person who carries out an occasional transaction is not a legal entity but a natural person. As a natural person cannot be owned by someone else, the obliged entity must establish, in relation to the natural person, whether the natural person wishes to establish a business relationship or to carry out a transaction 'in the interests, for the benefit or on behalf of' someone else.

business relationship with such a trust¹³⁵ cannot be established, as the person who actually wants to establish the business relationship or perform the act is a trust¹³⁶ that does not have legal capacity pursuant to Estonian law.

Differences in the case of civil law partnerships

- 4.3.1.31. The objective of identification of civil law partnerships¹³⁷ 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 the Guidelines and the objective of the business relationship or an occasional transaction must be ascertained according to point 4.3.6 of the Guidelines.
- 4.3.1.32. 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

- 4.3.1.33. The information and documents concerning the identification and verification of data are retained on the basis of clause 5 of the Guidelines.

4.3.2. **Identification of a legal entity**

General principles

- 4.3.2.1. Upon the establishment of a business relationship or the conclusion 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, including tools of e-identification and e-transaction trusts, using at least two sources for the verification of data in such a case.
- 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 the 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 service¹³⁸. 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 relationship¹³⁹. 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 (including the data collected upon 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 the Guidelines or that the business relationship should not be monitored within the meaning of point 4.4 of the Guidelines. Using

¹³⁵ Subsection 71 (1) of the MLTFPA. In English – *trust*.

¹³⁶ *Ibid*.

¹³⁷ See § 580 et seq. of the Law of Obligations Act about the legal nature of civil law partnerships.

¹³⁸ In the case of the limits specified in point 4.3.1.14 of the Guidelines, the total amount of all such outgoing payments must be cumulatively taken into account.

¹³⁹ 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.

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 the FSA, including 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 a 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 conclusion of the transaction or during the conclusion of the transactions.

Identification

- 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. the 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 the Guidelines;
- iv. contact details of the legal person;

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 establishment¹⁴⁰ must be proceeded from;
- ii. place of business of the legal entity¹⁴¹;

- 4.3.2.7. The following documents are used for identification:

- i. the registry card of the relevant register;
- ii. the registration certificate from the relevant register; or

¹⁴⁰ According to the theory of country of establishment, the location of a legal entity is the country in which the legal entity was established.

¹⁴¹ 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.

- iii. a document equivalent to the aforementioned document or relevant document of establishment¹⁴² of the legal entity.
- 4.3.2.8. If the original document specified in point 4.3.2.7 of the Guidelines cannot be seen, the obliged entity may use a copy of the document specified in point 4.3.2.7 of the Guidelines that has been authenticated by a notary, certified by a notary or officially certified or other information from a reliable and independent source, including means of e-identification and trust services of e-transactions, using at least two different sources for the verification of data.
- 4.3.2.9. 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

- 4.3.2.10. 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 the Guidelines are true and correct (the first four sub-points), also confirming¹⁴³ that the data directly related to the person (fifth 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 to be.

Reliable and independent source

- 4.3.2.11. 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 the Guidelines;
 - ii. sees a copy of the document specified in point 4.3.2.7 of the Guidelines that has been authenticated by a notary, certified by a notary or officially¹⁴⁴ certified;
 - iii. has access to the data in the Business Register, Register of Non-profit Associations and Foundations or the relevant registers of foreign countries via a computer network.
- 4.3.2.12. A document to be 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.
- 4.3.2.13. In situations not specified in point 4.3.2.11 of the Guidelines, the reliable and independent source is the verification of the information obtained upon identification, which (a) comes from two separate sources and (b) complies with the requirements specified in condition c of point 4.3.1.19 of the Guidelines. However, the provisions of point 4.3.2.11 of the Guidelines must be applied in situations where the representative of a legal entity must be

¹⁴² 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.

¹⁴³ 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.

¹⁴⁴ 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.

identified face-to-face according to point 4.3.1.14 of the Guidelines.

Two different sources

- 4.3.2.14. Within the meaning of point 4.3.2.13 of the 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).
- 4.3.2.15. In addition to the document¹⁴⁵ specified in point 4.3.2.7 of the 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

- 4.3.2.16. Public¹⁴⁶ documents issued in a foreign country must be legalised or confirmed with a certificate (an Apostille)¹⁴⁷, 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.
- 4.3.2.17. 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 document¹⁴⁸ (usually ministries of foreign affairs).
- 4.3.2.18. At the same time:
- i. public documents prepared or certified in countries with whom Estonia has entered into the relevant legal assistance agreement do not require legalisation or an Apostille;
 - ii. legalisation or an Apostille is not required for public documents issued in a country that implements the Convention Abolishing the Legalisation of Documents in the Member States of the European Communities.
- 4.3.2.19. 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).

¹⁴⁵ This document must always be one of the two sources.

¹⁴⁶ 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.

¹⁴⁷ 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.

¹⁴⁸ Further information about legalisation can be obtained from the website of the Estonian Ministry of Foreign Affairs (see (<https://www.vm.ee/konsulaar-viisa-ja-reisiinfo/konsulaarinfo-ja-teenused/dokumendi-legaliseerimine>), where documents issued in Estonia are also legalised.

Data retention

- 4.3.2.20. The information and documents concerning the identification and verification of data are retained on the basis of clause 5 of the 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 conclusion of an occasional transaction, the obliged entity must identify the beneficial owner of the customer or the person participating in the occasional transaction and implement measures to check 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. Beneficial owner means a natural person who has, either through ownership or other control, the ultimate dominant influence¹⁴⁹ over a natural or legal person, or in whose interests, for whose benefit or in whose name a transaction or action is made.
- 4.3.3.3. If the obliged entity establishes a business relationship with a customer whose beneficial owner information must be submitted to or registered in that country under the law of a Member State of the European Union, the obliged entity must receive an appropriate certificate of registration or an extract from the register of beneficial owner information.
- 4.3.3.4. 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 conclusion of an occasional transaction.
- 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 (including 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 the Guidelines or that the business relationship should not be monitored within the meaning of point 4.4 of the 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 to the FSA 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.

¹⁴⁹ The term 'dominant influence' is defined in § 27 of the Accounting Act. Dominant influence may, *inter alia*, arise from the following circumstances: 1) a holding of more than 50 per cent of the voting rights in the consolidated entity; 2) a direct or indirect right arising from law or a contract to appoint or remove the majority of the members of the executive management or the higher management body by exercising the rights of a founder or by a resolution of the general meeting. Dominant influence may also result from a personal, family, or contractual relationship.

Identification of the beneficial owner

- 4.3.3.7. The beneficial owner of a legal entity is identified in stages where the Obligated 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 manner¹⁵⁰, irrespective of the size of the shares, voting rights or ownership rights or its direct or indirect nature;
 - ii. whether it can be identified in whose interest, for the benefit of whom or in whose name a transaction or action is performed;
 - iii. 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 direct¹⁵¹ or indirect¹⁵² shareholding. Family¹⁵³ and contractual connections¹⁵⁴ must also be taken into account here;
 - iv. who is the natural person in senior management¹⁵⁵, who must be defined as the beneficial owner, as the answers to the previous questions have not made it possible for the obliged entity to identify the beneficial owner.
- 4.3.3.8. A member of senior management¹⁵⁶ specified in point 4.3.3.7 of the 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 day-to-day or regular management of the company (e.g. chief executive officer (CEO), chief financial officer (CFO), director or president).
- 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 person, the beneficial owner is the natural person who

¹⁵⁰ These may be situations where control is exercised via personal connections or 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.

¹⁵¹ A direct holding means that a natural person has a holding in a company personally.

¹⁵² An indirect holding means that a natural person has a holding in a company via one or multiple persons or a chain of persons. For example, in a situation where natural person X owns 50% of company A, which owns 100% of company B, which in turn owns 60% of company C, natural person X owns 30% of company C indirectly, thus being the beneficial owner of company C.

¹⁵³ If persons related via family ties (partners, descendants, ascendants, etc.) seem to be among the owners, it is necessary to check how much of the company belongs to the related persons.

¹⁵⁴ 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 to determine the size of the shareholding according to the scale of the actual control or influence.

¹⁵⁵ In English – senior management.

¹⁵⁶ The Ministry of Finance guidelines on the identification of beneficial owners include the recommendation in the case of managing bodies consisting of more than three people, the chairperson (or chairpersons as it's possible that two persons share this position) of the respective body is noted as the beneficial owner. If a person is noted as the beneficial owner due to their position as a member of a management body, this does not mean that they receive monetary income from the company or that the company operates in their personal interests. Online: <https://www.fin.ee/finantspoliitika-valissuhted/rahapesu-ja-terrorismi-rahastamise-tokestamine/tegeliku-kasusaaja>. (21.07.2023)

ultimately controls the association via direct or indirect ownership or otherwise and who is:

- i. the settlor of the trust or the founder of the association;
- ii. the trustee of the association;
- iii. the person ensuring and controlling the preservation of assets of the association, where such person has been appointed;
- iv. the beneficiary of the association, or where the beneficiary or beneficiaries are yet to be determined, the class of persons in whose main interest such association has been set up or operates; or
- v. any other person who in any way exercises ultimate control over the assets of the trust or association.

Verification of data

- 4.3.3.10. The obliged entity implements measures to check the identified beneficial owner and does the same to an extent that makes it possible for the obliged entity to be convinced of who the beneficial owner is.
- 4.3.3.11. The obliged entity verifies that the customers whose beneficial owner information must be submitted to or registered in that country under the law of a Member State of the European Union have done so according to the laws of their country of location. The obliged entity requires the customer to provide the relevant extract from the register or will obtain it directly from the register¹⁵⁷. Thus, the obliged entity verifies whether the customers who are obliged to disclose the beneficial ownership information have done so and whether it matches the information provided to the obliged entity.
- 4.3.3.12. In the case of identifying the purpose and nature of the business relationship, the obliged entity verifies 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, within the declared scope of activity and with the declared main business partners and has the required experience¹⁵⁸. The obliged entity:
 - i. sees the original of the document specified in point 4.3.2.7 of the Guidelines;
 - ii. has access to the data in the Business Register, Register of Non-profit Associations and Foundations or the relevant registers of foreign countries 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 the Guidelines that has been certified by a notary or officially certified;
 - iv. uses other publicly accessible and/or reliable sources.
- 4.3.3.13. In the case of customers not obliged to disclose information on beneficial owners¹⁵⁹ and if their identity documents or the other submitted documents do not indicate directly who the beneficial owner of the legal entity is, the relevant data (including data about being a member

¹⁵⁷ Legal entities registered in Estonia are required to disclose the information on their beneficial owners to the Business Register in accordance with § 76 et seq. of the MLTFPA.

¹⁵⁸ See also points 4.3.6.24 to 4.3.6.27 of the Guidelines.

¹⁵⁹ Legal entities and trusts registered in EU countries are obliged to disclose information on beneficial owners.

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 implement reasonable measures to verify the submitted information.

- 4.3.3.14. 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 4.3.3.13 of the 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

- 4.3.3.15. 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, including it is in contravention of the data obtained in the course of identification of the beneficial owner and the verification of data.

Data retention

- 4.3.3.16. 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 information and documents are retained on the basis of clause 5 of the 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 event¹⁶⁰ occurs, the obliged entity will implement 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 (including high-risk politically exposed person), their family member or close associate, or if the customer has become such a person.
- 4.3.4.2. Politically exposed person (PEP) means a natural person who performs or has performed prominent public functions and with regard to whom related risks remain. At least the following positions are deemed to perform prominent public functions: head of state or head of government; minister, deputy minister or assistant minister; member of a legislative body; member of a governing body of a political party; judge of the highest court of a country; auditor general or a member of the supervisory board or executive board of a central bank; the chancellor of justice; ambassador, envoy or chargé d'affaires; high-ranking officer in the armed forces; member of an administrative, management or supervisory body of a state-owned enterprise; director, deputy director and member of a management body of an international organisation or a person performing similar functions, who does not have the status of a middle-ranking or more junior official. A person who, as per the list published by the European Commission, is considered a performer of prominent public functions by a Member State of the European Union, the European Commission or an international

¹⁶⁰ In English – trigger event.

organization accredited on the territory of the European Union is deemed a politically exposed person¹⁶¹.

- 4.3.4.3. The obliged entity applies the measures specified in point 4.3.4.15 of the Guidelines to high-risk politically exposed persons.
- 4.3.4.4. 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

- 4.3.4.5. For the purposes of the Guidelines, a high-risk politically exposed person is any politically exposed person, a member of their family or a close associate, unless the person is from, resides in or is established in a country that is a contracting party to the EEA Agreement and there are no indications of a higher risk¹⁶².
- 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 implement 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 implement 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. 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.
- 4.3.4.8. 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 function¹⁶³ 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)¹⁶⁴ authorisation over the state's assets or funds or policies or activities, whether they have the right to issue licences or permits or make exceptions, whether they have control or influence over the accounts or funds of the state or the company, etc.

Family member

- 4.3.4.9. A family member means the spouse, or a person considered to be equivalent to a spouse, of the politically exposed person; a child of the politically exposed person and the child's spouse, or a person considered to be equivalent to a spouse; and a parent of the politically exposed

¹⁶¹ The list of posts in Estonia, including accredited international organisations located in Estonia, whose holders are considered to be politically exposed persons, is established by Minister of Finance Regulation No. 34 of 22.09.2020 'List of positions in Estonia the holders of which are considered politically exposed persons'. - RT I, 14.10.2022, 2.

¹⁶² The provisions of point 4.2 of the Guidelines must be taken into account upon risk assessment.

¹⁶³ I.e. owns a function that is not associated with middle-ranking or more junior officials.

¹⁶⁴ In English – substantial.

person.

Close associate

4.3.4.10. A close associate¹⁶⁵ means a natural person who is known to:

- i. have joint beneficial ownership of a legal person or trust with a politically exposed person;
- ii. have close business relations with a politically exposed person;
- iii. be the beneficial owner of a legal person or trust set up in the interests of a politically exposed person¹⁶⁶.

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

4.3.4.11. 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 databases¹⁶⁷) that provide the relevant service;
- ii. asking the representative (covers asking the representative and beneficial owner or their family members and close associates) or the person concluding an occasional transaction about the status of a politically exposed person, also asking the customer or the person concluding an occasionally concluded transaction about their profession or area of activity and requesting 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.

4.3.4.12. Sub-point 2 of point 4.3.4.11 of the Guidelines must be applied generally¹⁶⁸ and sub-point 3 must be applied when¹⁶⁹ sub-point 1 is not applied. As a result of the risk-based approach, the obliged entity may also implement additional measures in comparison with the measures specified in point 4.3.4.11. 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.

4.3.4.13. The measures implemented to identify a high-risk politically exposed person must be risk-based, i.e. comply with the size of the obliged entity and the nature, scope and level of

¹⁶⁵ 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).

¹⁶⁶ A trust or legal entity can be created for the benefit of a politically exposed person, without the politically exposed person being its beneficial owner. For example, where a trust or legal entity is set up to organise election or media campaigns in support of the politically exposed person.

¹⁶⁷ This must correspond to the fuzzy match principle, i.e. a 100% match of the name is not necessary, and measures must be implemented to check matches of less than 100%. The obliged entity must make sure whether this is the same person or not.

¹⁶⁸ Except if the obliged entity is convinced that the person cannot be a 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 ask about the profession or area of activity). However, the obliged entity is prepared to explain how they knew that the person was not a (high-risk) politically exposed person and why the person was therefore not asked if they are a politically exposed person.

¹⁶⁹ Except in the case provided for in the preceding footnote.

complexity of the activities and services provided, including 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 proceeds¹⁷⁰ or finance terrorism or proliferation¹⁷¹ via the services provided by the obliged entity, the more or the more extensive measures the obliged entity must implement from among the measures specified in point 4.3.4.11 of the Guidelines (in conjunction with point 4.3.4.12 of the Guidelines).

- 4.3.4.14. In any case, the obliged entity is ready to justify to the FSA 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 4.3.4.13 of the Guidelines are not present.

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

- 4.3.4.15. In addition to the general due diligence measures specified in point 4.3 of the Guidelines, the obliged entity applies the following due diligence measures to high-risk politically exposed person:
- i. obtains approval from the senior management to establish or continue a business relationship with the person;
 - ii. applies measures to identify the source and/or origin of the wealth of the person and the sources of the funds used in the business relationship or for the occasional conclusion of transactions.
 - iii. monitors the business relationship in an enhanced manner within the meaning of point 4.4 of the Guidelines (see also point 4.6 of the Guidelines).
- 4.3.4.16. The source and/or origin of wealth is something other than the source and origin of the funds used in a transaction (compare the following with point 4.4.3 of the 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 altogether 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, register of companies, etc. If the risk related to the customer is high, the data of the source and/or origin of wealth must be checked on the basis of reliable and independent data, documents and information. 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) 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 to the higher risk to which enhanced attention must be given, i.e. about which enhanced measures must be implemented.

¹⁷⁰ See also Annex 1 to the Guidelines.

¹⁷¹ See also Annex 2 to the Guidelines.

Data retention

4.3.4.17. The obliged entity registers and retains information about all actions taken to identify a politically exposed person, including the considerations about the determination or non-determination of their 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 the Guidelines.

4.3.5. **Identification of the source and/or origin of wealth**

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, and 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 concluded 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 the Guidelines) in the appropriate case. The obliged entity also implements 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 the 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 4.3.4.16 of the 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 occasional transaction. This is only one, but a significant, part of the implementation of the Know Your Customer principle¹⁷². In doing so, the obliged entity must identify the permanent address, place of business or residence of the customer or participant in the occasional transaction, the occupation or profession, main transaction partners, payment practices and whether the obliged entity is acting for or on behalf of another person and, experience in the case of a legal entity.

4.3.6.2. In the appropriate case, the obliged entity must implement 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) the risk and/or risk profile associated with the customer and 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 implemented in appropriate case

4.3.6.3. The additional measure specified in point 4.3.6.2 of the Guideline is, *inter alia*, making queries in public sources¹⁷³ and additional information is the identification of the permanent address, place of business or residence of the customer or participant in the occasional transaction,

¹⁷² See also point 4.1.4.2 of these Guidelines.

¹⁷³ Internet searches, use of Google Maps to find information about the place of business, etc.

the occupation or profession¹⁷⁴, main transaction partners, payment practices and whether the obliged entity is acting for or on behalf of another person and, experience in the case of a legal entity. The above is not an exhaustive list and, if necessary, the obliged entity implements additional measures to understand the purpose and nature of the business relationship, including primarily identifies the source and/or origin of wealth, and if necessary, visits the site before the establishment of the business relationship¹⁷⁵, etc. In the case of certain services, the aforementioned circumstances can be partially or fully ascertained in 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 of realisation of an investment).

- 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, including the person, the beneficial owners and the customer profile. Also, the reason why a particular service is needed. The obliged entity must make 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 of the customer. The obliged entity must assess on the basis of said 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 on the basis of the information already collected (to constantly observe/monitor the transactions concluded within the business relationship, including 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 a sanctioned person or that the transactions of the customer are attempts to avoid a 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 the 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. Thus, the identification of the purpose and nature cannot be limited to the mere collection of information because this does not 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 to which the customer performs transactions in the course of the business relationship. The important 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 in this area of activity to conclude transactions with these business volumes and have 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

¹⁷⁴ Including ascertaining that an authorisation or registration exists.

¹⁷⁵ The purpose is to understand whether the information submitted by the customer corresponds to reality.

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 purposes of the transactions are (including that a fictitious intermediary has not been created for the purpose of transferring funds), whether the Internet bank solution will be logged in from the same IP addresses (who this person is and why one person manages all of the transactions). It must also 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 the 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 the NRA and Annexes 1 and 2 of the Guidelines and to implement the relevant measures. The obliged entity must keep in mind that several characteristics that refer to risks together or separately may be a sign of the use of a shell company¹⁷⁶ or of other suspicious and unusual activity that is in conflict with reasonable economic activities. In this case the obliged entity must also explain to the FSA, where necessary, why the obliged entity has established a business relationship that corresponds to such characteristics and why it is continued.
- 4.3.6.8. As is the case with all other due diligence measures, the risk-based approach stipulated in point 4.2 of the 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 implement 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 and why, i.e. whether this wish corresponds to their actual activities, capacity and needs. In such cases, general information is not enough¹⁷⁷.
- 4.3.6.9. The additional measures and exceptions concerning life insurance companies, creditors and credit intermediaries and fund management companies have been specified in points 4.7.1, 4.7.2 and 4.7.3 of the Guidelines, respectively.

Area of activity

- 4.3.6.10. In order to identify the customer's 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. Also 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 gaining an

¹⁷⁶ 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.

¹⁷⁷ This means that information (including about transactions) may not be vague, i.e. based on an abstract description. In the case of an abstract description, the obliged entity cannot study the data in depth and ensure that they know the customer and have an adequate overview 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.

understanding of what the customer is doing and the retention of these 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, they may not be economically unreasonably too broad¹⁷⁸ or completely different from each other¹⁷⁹, which would allow the customer to basically deal with everything, and it would therefore be impossible for the obliged entity to correctly monitor the business relationship later.
- 4.3.6.12. Upon identification of the area of activity, the obliged entity must also ascertain whether the customer has the authorisation or registration necessary for the provision of the service 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 the Guidelines).
- 4.3.6.13. All in all, the identification of the customer's 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 the Guidelines and allow for these circumstances to be identified.

Payment practices

- 4.3.6.14. The verification of payment practices must be based on the service provided by the obliged entity and the risk of the customer. It is important to identify the manner in which financial services are consumed, including for example (i) the approximate number, volume, purpose and frequency of transactions concluded per month and per year, the countries from which payments are received and to which payments are made, the expected duration of the business relationship, the extent and channels of cash use, payment channels (branch, Internet bank, card payments), etc.¹⁸⁰; (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 the Guidelines.
- 4.3.6.15. The obliged entity must thereby ascertain whether, why and on which conditions the customer is capable of concluding such transactions¹⁸¹ and how this corresponds to the customer's knowledge in other respects, including with 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.

¹⁷⁸ 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 selling and buying basically everything.

¹⁷⁹ For example, the 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).

¹⁸⁰ In appropriate cases, 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.

¹⁸¹ For example, requesting an annual report and comparing the data therein with the planned activities may also be relevant.

- 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 the 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 volumes, i.e. who are the persons who will realise the purpose of the establishment of the business relationship.
- 4.3.6.18. The main business partners means the persons who make the conclusion of incoming and outgoing transactions possible¹⁸², 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, primarily in the case of a risk that is higher than usual, also identify how these main business partners are associated with the area of activity, i.e. whether the information that also confirms operation in this area of activity is publicly accessible. The obliged entity must ascertain in the appropriate case why these main business partners agree or are prepared (including on which preconditions¹⁸³) 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 company¹⁸⁴ 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 the purchase or sale of goods, asking about main business partners covers in the appropriate case (primarily in the case of a risk that is higher than usual), asking about service providers that transport goods.
- 4.3.6.21. It is important in the appropriate case (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 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 the Guidelines and allow for these circumstances to be identified.

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

- 4.3.6.24. The customer's area of activity, payment practices and main business partners must correspond to the experience profile of the customer's representative (or key persons) and/or the beneficial owner. This often requires identifying the source and/or origin of the

¹⁸² For example, in the case of the purchase and sale of goods, who the persons from whom goods are purchased are and to whom they are sold.

¹⁸³ For example, prepayments, etc. and the actual compliance with their preconditions.

¹⁸⁴ In English – shelf company.

client's wealth more generally.

- 4.3.6.25. The obliged entity must 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 cannot be limited to requesting CVs but requires an understanding and analysis of how the customer's previous knowledge fits into the business activity¹⁸⁵. 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 the 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

- 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 events¹⁸⁶, i.e. primarily the data concerning the person, their representative (including 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 checked 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, excluding the assessment of the risk profile of a high-risk customer, which must be assessed again six months after the establishment of the business relationship.
- 4.4.1.3. The obliged entity decides on 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 methods without having to intervene in the usual functioning of the customer relationship¹⁸⁷.

¹⁸⁵ 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.

¹⁸⁶ In English – trigger event.

¹⁸⁷ For example, in the case of a lower or medium-risk natural person who is a regular consumer of a service, it may be appropriate to update the data using indirect methods, based on information collected in the context of business relationship monitoring on the payment discipline of the person, where the regularity of transactions on the accounts, etc. does not give

4.4.2. Business relationship monitoring

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. Business relationship monitoring covers the entire business relationship of the customer and its life cycle, including 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 constant monitoring of a business relationship, the obliged entity must monitor the transactions concluded during the business relationship in such a manner that it can determine whether the transactions 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 in order to identify the customer's activity or circumstances indicating criminal activity, money laundering or terrorist financing or likely to be linked to money laundering or terrorist financing. Including 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.
- 4.4.2.3. In the course of the business relationship, the obliged entity must also constantly assess the changes in the customer's activities and assess whether the risk level associated with the customer and the business relationship may increase and whether the need to apply additional or enhanced due diligence measures arises, including in a 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. The obliged entity constantly assesses whether the purpose and nature of each single transaction correspond to what was ascertained in the course of the application of due diligence measures upon the establishment of the business relationship, i.e. the information previously known about the 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, including 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 upon the application of all other due diligence measures, the risk-based approach stipulated in point 4.2 of the Guidelines must be proceeded from here as well. The higher the risk/threat associated with the customer, the more the obliged entity must implement 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. The information cannot be vague¹⁸⁸.

reason to believe that the information collected when the business relationship was established has changed (the person is still receiving a salary or pension from the same place, the person is still going to the grocery shops in the same town or paying the same person for utilities, etc., i.e. the person's place of residence and the source of funds have remained the same).

¹⁸⁸ This means that information (including information about transactions) may not be vague, i.e. based on an abstract

- 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 constant 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 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 4.1.7.4 and 4.1.7.5 of the Guidelines. This is the same situation as the one where the obliged entity had not applied due diligence measures from the beginning.
- 4.4.2.7. The obliged entity acknowledges and implements measures to identify in the course of the monitoring of the business relationship, among others, whether the customer in the business relationship is the person that they claim 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 companies, creditors and credit intermediaries and fund management companies have thereby been specified in points 4.7.1, 4.7.2 and 4.7.3 of the Guidelines, respectively.
- 4.4.2.9. Transaction monitoring measures are divided into two categories: Measures that can be used to monitor (screen¹⁸⁹) 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 (monitor¹⁹⁰) transactions later.
- 4.4.2.10. The objective of monitoring the business relationship is, *inter alia*, to identify the circumstances referring to the risks specified in the NRA and in Annexes 1 and 2 of the Guidelines and the implementation of relevant measures. The obliged entity must keep in mind that several characteristics that refer to risks together or also separately may be a sign of the use of a shell company¹⁹¹ or of other suspicious and unusual economic activities, where the obliged entity must, where necessary, explain to the FSA why it has established and continues a business relationship that corresponds to such characteristics.

Screening

- 4.4.2.11. Screening 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 question¹⁹² is an important part of the due diligence measures implemented by obliged entities. This makes it possible to identify circumstances

description. In the case of an abstract description, the obliged entity 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 an overview of the customer that would allow 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.

¹⁸⁹ In English – screening.

¹⁹⁰ In English – monitoring.

¹⁹¹ 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.

¹⁹² 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.

in the economic activities of customers that may refer to money laundering and terrorist financing. The screening of business relationships for the aforementioned purposes also has a role in the identification of subjects of possible sanctions or transactions restricted with sanctions and politically exposed persons.

- 4.4.2.12. According to the screening of transactions in real time, employees (see point 3.7 of the Guidelines about roles) screen the customer's behaviour and transactions upon the performance of their tasks in order to identify (i) suspicious and unusual transactions and transaction patterns, (ii) transactions that exceed the established limits, or (iii) politically exposed persons and circumstances related to sanctions.
- 4.4.2.13. The obliged entity can do the following to screen business relationships and transactions in real time:
- 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 the obligation to review transactions manually; or
 - iii. use a combination of the above two measures.
- 4.4.2.14. The measures implemented to screen a business relationship in real time must be proportional and risk-based, i.e. comply with the obliged entity's size, activities and the nature, scope and complexity of the services provided, including the risk appetite and risks arising from the activities of the obliged entity. This means that the bigger the customer base of the obliged entity (the obliged entity cannot screen transactions manually) and the higher the risk that criminal proceeds may be legalised (i.e. laundered)¹⁹³ or terrorism and proliferation may be financed¹⁹⁴ via the services provided by the obliged entity, the more or the more extensive measures the obliged entity must implement according to point 4.4.2.13¹⁹⁵ of the Guidelines.
- 4.4.2.15. If the obliged entity uses automatic IT systems to identify suspicious and unusual transactions carried out within the scope of specific business relationships, it should ensure that these systems are expedient, i.e. they comply with the obliged entity's size, activity and the nature, scope and level of complexity of the activities and services provided, including the risk appetite and risks arising from activities of the obliged entity.
- 4.4.2.16. Considering that the purpose of screening business relationships in real time is to identify (i) suspicious and unusual transactions and transaction patterns, (ii) transactions that exceed the established limits, or (iii) politically exposed persons and circumstances related to 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 (including 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, including are areas of conflict, or from countries that have other important

¹⁹³ See also Annex 1 to the Guidelines.

¹⁹⁴ See also Annex 2 to the Guidelines.

¹⁹⁵ Proportionality and a risk-based approach regarding the measures to be taken to screen the business relationship and transactions in real time also means, *inter alia*, that the level of automation of the solution used will depend on the business model of the obliged entity, including business volumes and the digitalisation of the products or services offered.

connections with the aforementioned countries;

- iii. also cover the descriptions of transactions and the information therein;
- iv. there is the capacity to check the customer, the customer's representative and the beneficial owner to identify a subject of a sanction¹⁹⁶;
- v. in order to identify politically exposed persons, cover the capacity to verify the compliance of the data of the customer, the customer's representative and the beneficial owner¹⁹⁷;
- vi. guarantee the identification of persons (cover the person themselves and 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 cancelled (including 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 for the obliged entity to implement measures if the same persons want to establish a business relationship again;
- vii. ensure the possibilities 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 the Guidelines).

4.4.2.17. Upon the selection of an automatic IT system, the obliged entity must ensure that such screening takes place at least once a week, excluding sub-points 1-3 of point 4.4.2.16 of the Guidelines, which has to take place in real time. Also excluding sub-point 4, which must also take place in real time if the obliged entity does not take measures every time changes are made in sanctions.

4.4.2.18. When selecting an automated IT system, the obliged entity must organise regular and needs-based tests for checking its effectiveness and for the management and mitigation of identified risks.

4.4.2.19. If the obliged entity does not select an appropriate IT system, the manual review systems must comply with the principles of point 4.4.2.16 of the Guidelines.

4.4.2.20. The obliged entity is ready to justify to the FSA why the obliged entity selected such a solution for screening business relationships and why the circumstances and risks specified in point 4.4.2.14 of the Guidelines are not present. The obliged entity is also ready to justify why it has selected the specific parameters/case scenarios.

Monitoring

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

¹⁹⁶ The obliged entity must thereby consider the extent to which the data collected during general due diligence measures (including the data collected in the course of screening) are relied on or the extent 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.

¹⁹⁷ *Ibid.*

- 4.4.2.22. In order to monitor transactions, employees (see point 3.7 of these Guidelines for roles) observe the customer's behaviour and transactions upon the performance of their tasks in order to identify transactions and circumstances that could not be identified in real time (they could not be intervened in) 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).
- 4.4.2.23. Below are examples of some typical parameters¹⁹⁸ 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) customers with larger turnovers in the period under review, users of the service, 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 carried out in the period under review that exceed a certain limit;
 - iv. cash transactions that exceed a certain limit (by natural persons and legal entities);
 - v. unexpected increase in the turnover of VOSTRO accounts in correspondent relationships¹⁹⁹;
 - vi. transactions of a certain customer (type).

Transactions indicating higher risk

- 4.4.2.24. Pursuant to point 4.2.7.5 of the Guidelines, the obliged entity must pay enhanced attention or apply enhanced due diligence measures to transactions and transaction patterns that are complicated, high-value and unusual and that have no reasonable or obvious economic or legitimate purpose or are uncharacteristic of the specific features of the business in question.
- 4.4.2.25. In addition to the application of enhanced due diligence measures, the background of each single transaction specified in point 4.4.2.24 of the Guidelines must be investigated to the extent that is reasonably necessary, including 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. The main circumstances to which attention must be given in analysing such transactions are as follows:
- i. what is suspicious about the operations, transactions or other circumstances;
 - ii. whether the obliged entity is convinced that they know the customer to the necessary extent and whether the customer's activity corresponds 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 implemented to understand the background and purpose of the transaction. For example, by identifying the source and destination of the funds or looking for more information

¹⁹⁸ The obliged entity may also use other principles of transaction monitoring.

¹⁹⁹ Including in those that are not high-risk correspondent relationships.

about the customer's activities in order to identify that such a transaction is true;

- iii. whether there have been repeated signs of suspicious operations and transactions (including 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, including to details;
- v. whether the obligation to report to the FIU must be performed within the meaning of point 7 of the Guidelines.

Customer visits

- 4.4.2.26. 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 does not perform on-site visits to the customer to check whether the customer's explanations of their capability and capacity are true. 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

- 4.4.2.27. The obliged entity registers and retains information about all actions carried out, i.e. checks whether the transactions concluded correspond to what the obliged entity knew about the customer beforehand. This covers the investigation of transactions that have been described in point 4.4.2.24 of the 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 the Guidelines.

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

General principles

- 4.4.3.1. Within the scope 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 the 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 the Guidelines apply to the source and origin of the funds used in the transaction.
- 4.4.3.3. The explanations in the general principles of point 4.4.2 of the Guidelines, which explain the scope of the application of due diligence measures, i.e. which characteristics the collected information must correspond to (including 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 constant, 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, including 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) for 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 the Guidelines).
- 4.4.3.6. 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 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 for the reason that 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 the Guidelines), the identification of the source and origin of the funds used in the transaction requires the 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 actions 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 the 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 the Guidelines that the risk of money laundering or terrorist financing in the case of the customer and their activities is lower (smaller) 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 or action carried out by the customer during the business relationship or in the case of an occasional transaction.

4.5.5. Simplified due diligence measures may be applied during a business relationship if circumstances characteristic of a lower risk have been established and at least the following conditions have thereby 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 Business Register in Estonia or in a branch of a foreign credit institution or in a credit institution that was established or whose place of business is in a Contracting State of the European Economic Area or in a state where requirements equivalent to those stipulated in the relevant directives of the European Parliament and of the Council²⁰⁰ are implemented;

4.5.5.3. a limit has been established for the total value of incoming or outgoing transactions.

4.5.6. The obliged entity considers the provisions of the EBS Guidelines on risk factors²⁰¹ 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. also checking 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 checked).

4.5.6.2. in the course of the constant 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

²⁰⁰ See footnote 104 for the relevant directive of the European Parliament and of the Council.

²⁰¹ See footnote 36.

if a certain trigger event²⁰² 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 obliged entity 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 the Guidelines) and make it possible to report to the FIU on suspicious transactions (see also point 7 of the Guidelines).

4.5.8. The information collected during the application of simplified due diligence measures to a customer must give the obliged entity 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, *inter alia*, the money laundering and terrorist financing risks and methods characteristic of Estonia given in Annexes 1 and 2 to the Guidelines.

4.5.10. The obliged entity documents and, upon the demand of the competent supervisory authority, explains why, in respect of what and which simplified due diligence measures the obliged entity has applied to the customer upon the establishment of the business relationship or to transactions within the scope of 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 the Guidelines that the risk of money laundering or terrorist financing in the case of the customer and their activities is higher (bigger) 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 ordinary mandatory due diligence measures.

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

4.6.6. When deciding on enhanced measures in respect of the customer or their transaction, the obliged entity takes into account the provisions of the EBA Guidelines on risk factors²⁰³, whilst the reassessment of the customer's risk profile six months after the establishment of the business relationship is always an enhanced due diligence measure. Enhanced due diligence measures may, among others, also be

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

²⁰² In English – trigger event.

²⁰³ See footnote 36.

- i. identification of all beneficial owners of the company (including those whose shareholding is below 25%);
- ii. carrying out an independent assessment of the customer and, if necessary, requesting 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 constant monitoring of the business relationship:

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

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

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 the Guidelines must be applied in the case of a correspondent relationship with a respondent institution from a high-risk or third country and high-risk third parties.

4.6.9. The obliged entity documents and, upon the demand of the competent supervisory authority, explains why, in respect of what and which enhanced due diligence measures the obliged entity has applied to the customer upon the establishment of the business relationship or to transactions within the scope of the business relationship.

4.7. Special cases of due diligence measures²⁰⁴

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.

²⁰⁴ In cases not covered by point 4.7 of the Guidelines, but also in addition in the specific cases set out in point 4.7, the obliged person must, when applying due diligence measures, take into account, *inter alia*, the relevant sectoral guidance contained in Section II of the EBA Guidelines on risk factors (see footnote 36), which is relevant to the specific business model, products and services offered.

- 4.7.1.2. In the case of life insurance products, the obliged entity applies due diligence measures not only to the customer and the beneficial owner but also to the beneficiaries.
- 4.7.1.3. The name of the person named as the beneficiary, including if a natural person, legal entity or unit has been identified as the beneficiary, must be identified immediately after the determination of the person or after learning of the person. If the obliged entity knows that the beneficiary is a third party, the beneficial owner of the beneficiary is also identified at the time of naming.
- 4.7.1.4. Where the beneficiary is not determined by name, but based on certain characteristics²⁰⁵ or in another manner, sufficient data must be gathered on the circle 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 making a payment.
- 4.7.1.5. The identity of beneficiaries is verified at the time of making a payment. Points 4.3.1 and 4.3.2 of the 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).
- 4.7.1.6. 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 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 the 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.
- 4.7.1.7. 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 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 4.7.1.6 of the 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 their close associate in addition to the beneficiary. The requirements stipulated in point 4.7.1.6 of the Guidelines must be implemented if such circumstances are ascertained in order to check the business relationship and inform the management board about the identification (see also point 4.3.4 of the Guidelines).
- 4.7.1.8. 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.
- 4.7.1.9. 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

²⁰⁵ In English – class of beneficiaries.

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 the 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, including at the level of contracts, for relying on another person must be complied with (see point 4.8.2 of the 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 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 authorisation²⁰⁶, 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 the 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, including at the level of contracts, for relying on another person must be

²⁰⁶ This point applies to situations where the creditor is a licensed creditor and the case is not that of peer-to-peer loan intermediation.

complied with (see point 4.8.2 of the 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.
- 4.7.3.3. The obliged entity takes appropriate measures to determine the money laundering and terrorist financing risk of the investment and applies enhanced due diligence measures in higher risk situations and simplified due diligence measures in lower risk situations before making the investment.

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 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 establish 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, including 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 (including 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, including 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 the 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 where the obliged entity is a member; 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 the Guidelines cannot be outsourced. This restriction does not apply to outsourcing activities related to the identification and implementation of sanctions.²⁰⁷
- 4.8.1.6. The obliged entity selects the other person specified in the point 4.8.1.4 with due diligence to ensure the capacity of this person to comply with the requirements of the MLTFPA and these Guidelines, and the reliability and necessary qualification of this person. When outsourcing the activity (activities) of the obliged entity, the obliged entity must ensure that the other person has the required knowledge and skills, primarily for identifying suspicious and unusual situations, and that they are capable of complying with all of the money laundering and terrorist financing prevention requirements stipulated by legislation. In order to comply with this point, the obliged entity must make sure that the managers of the other entity are informed about these requirements and ensure the training of employees on the prevention of money laundering and terrorist financing within the scope described in point 3.9 of the 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. the division of the rights and obligations associated with outsourcing, including 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 the performance of the obligations provided for in the MLTFPA and these

²⁰⁷ 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.

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 the 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, including by way of an on-site inspection or another supervisory measure;
 - vi. the required level of knowledge, skills and capacity of the other person and the set of measures implemented for this purpose, including regular training;
 - vii. that the obliged entity has the unrestricted right to inspect compliance with the requirements of 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, that 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 supervisory authority immediately. The contract must guarantee that any information that is relevant upon 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 upon 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 the FSA 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 the 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, the obliged entity also proceeds from the FSA's advisory guidelines 'Requirements for Outsourcing by Persons Subject to Financial Supervision'²⁰⁸ and the EBA

²⁰⁸ Applies to all obliged entities except credit institutions, investment firms, payment institutions and e-money institutions.

Guidelines on outsourcing²⁰⁹.

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 if the obliged entity:

- i. gathers from the third party at least information on the person establishing the business relationship or making the transaction, their representative and the beneficial owner as well as 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 complies with requirements equal to those established in the relevant directives of the European Parliament and of the Council²¹⁰, 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 implements adequate measures to ensure performance of the obligations stipulated in point 4.8.2.2 of the Guidelines, including 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.

4.8.3. Failure to apply due diligence measures to ultimate beneficial owners in correspondent relationships

4.8.3.1. If the obliged entity provides a service to another credit or financial institution within the scope of a correspondent relationship²¹¹ 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

Online: <https://www.fi.ee/et/juhendid/pangandus-ja-krediit/nouded-finantsjarelevalve-subjekti-poolt-tegevuse-edasiandmisele-outsourcing-uus-redaktsioon>. (21.07.2023)

²⁰⁹ EBA 'Guidelines on outsourcing arrangements' of 25.02.2019, issues as advisory guidelines of the FSA on the basis of FSA Management Board Resolution No. 1.1-7/92 of 05.08.2019. Online: https://www.fi.ee/sites/default/files/2019-08/pp%20nr%2004%20EBA%20Tegevuse%20edasiandmise%20suunised%20ET_0.pdf. (21.07.2023). The Guidelines apply to credit institutions, payment institutions and e-money institutions.

²¹⁰ See footnote 102 for the relevant directive of the European Parliament and of the Council.

²¹¹ Defined in § 7 of the MLTFPA.

upon performance of the obligations stipulated in point 4.9.6²¹² of the Guidelines, if the obliged entity:

- i. has ascertained that the credit or financial institution that is a customer (i) is itself obliged to apply and does in practice apply measures equivalent to the requirements set out in the MLTFPA, including the application of due diligence measures, the identification of politically exposed persons and data retention requirements, (ii) is subject to financial supervision, and (iii) takes adequate measures to ensure compliance with the above conditions;
- ii. is aware of the risk structure of the customers that are the final beneficiaries²¹³ and monitors that the associated risk corresponds to the risk appetite of the obliged entity;
- iii. has guaranteed with a contract that, where necessary, it immediately obtains all data and documents in order to identify the person who ultimately benefits from the transaction.

4.8.3.2. The obliged entity is responsible for compliance with the requirements of 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 4.9.6²¹⁴ of the 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 approach in the case of any correspondent relationship²¹⁵ in order to identify suspicious and unusual transactions of the respondent institution²¹⁶ and their customers. Also what the code of conduct of the correspondent institution upon the identification of said transactions is like.

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 conclusion of 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 institution²¹⁷ 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

²¹² Excluding point 4.9.6.8 if the institution is not a respondent institution of a high-risk or a third country.

²¹³ The type and size of the risks to which the obliged entity is actually exposed in the correspondent relationship through the customers that are the final beneficiaries and their transactions.

²¹⁴ Excluding the exception specified in the previous footnote.

²¹⁵ See § 7 of the MLTFPA for the definition of a correspondent relationship.

²¹⁶ I.e. with a respondent institution outside the European Union.

²¹⁷ 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.

entities of high-risk third countries, makes changes to them if necessary or terminates these business relationships.

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-risk²¹⁸ or third country respondent institution, in which case the obligations stipulated in point 4.9.6 of the 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 respondent institution of a country with a higher risk of money laundering or terrorist financing or third country 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 the Guidelines on enhanced due diligence measures):

4.9.6.1. collect sufficient 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 risks²¹⁹ 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. must have established that the respondent institution is under financial supervision. Collect adequate information about the quality of supervision, including 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. must have ascertained that the respondent institution has an appropriate organisational solution for the prevention of money laundering and terrorist financing, implementation of sanctions and forwarding of information related to payments. Also ascertained that the respondent institution is obliged to apply and actually applies measures equal to those established in the relevant directives of the European Parliament and of the Council²²⁰, including the requirements to apply due diligence measures and retain data. The obliged entity implements adequate measures and, among others, assesses the control systems of money laundering and terrorist financing prevention implemented 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, including the risks arising from activities. Such assessment may occur as an on-site or remote inspection of the respondent institution;

4.9.6.4. be aware of the risk structure of the customers that are the final beneficiaries. Also 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. make sure in the case of payables through accounts²²¹ that the respondent institution has checked the identity of the customers who have direct access to the accounts of the correspondent institution, constantly implements due diligence measures for them and manages to present the appropriate due diligence measures to be implemented for the

²¹⁸ In any case, a high-risk respondent institution is an institution that is granted the right to use payable through accounts (see also footnote 218).

²¹⁹ 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 the associated risks, including 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.

²²⁰ See footnote 102 for the relevant directive of the European Parliament and of the Council.

²²¹ In English – payable through accounts.

customer if requested;

- 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 the Guidelines are concerned, including apply the business relationship monitoring measures specified in point 4.4 of the Guidelines and, if necessary, other appropriate measures;
 - 4.9.6.7. document or determine by a contract or any other mutual agreement the relevant rights²²² and obligations of both institutions in the correspondent relationship, including 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 existing at 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 (including if the respondent institution is a parent company via whom the subsidiary also uses the services of the correspondent institution), the circumstances specified in points 4.9.6.1 to 4.9.6.6 of the 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 the Guidelines and the EBA Guidelines on risk factors²²³ (especially Guideline 8 of Section II) and the relevant risk factors specified in the documents mentioned therein.
- 4.9.10. If the obliged entity, as a correspondent institution, uses the questionnaires prepared by international organisations²²⁴, it must assess whether this is sufficient to fulfil its obligations under the MLTFPA and the Guidelines and, if necessary, implement additional measures.

4.10. Transactions with natural persons and legal entities operating in high-risk third countries, including FATF high-risk countries

- 4.10.1. If the obliged entity has contact²²⁵ with a high-risk third country via a transaction carried out in their

²²² Including 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.

²²³ See footnote 36.

²²⁴ For example, the respective questionnaires of the Wolfsberg Group (e.g. *Correspondent Banking Due Diligence Questionnaire* (CBDDQ)).

²²⁵ Having contact may mean 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. A business relationship or transaction always involves a high-risk third country if: the funds were created or received in that country; the funds are held in that country; the transactions are with a natural person or legal entity resident or established in that country; or the transactions are with a trustee or trust established in that country and governed by the law of a high-risk third country. Enhanced due diligence measures will also apply if: the transaction transits through that country, e.g. because of the location of the payment service intermediary, or the customer's beneficial owner is resident in that country. In addition, the risks associated with the business relationship and the transaction must be assessed if it is known that the client

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 on the purpose of planned or executed transactions;
 - 4.10.1.5. receiving permission from the senior management to establish or continue a business relationship;
 - 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 or transaction patterns 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 the 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, including the FATF high-risk countries. The obliged entity applies these countermeasures and ensures that these measures are effective and proportional to the risks taken.

5. Registration and retention of data

- 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 conclusion of an occasional transaction by the obliged entity on the basis of point 6.1.1 of the Guidelines;
 - 5.1.2. information if it is impossible to implement 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, including 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. The obliged entity is not required to register and retain originals or copies of documents on which the identification and the verification of the information provided are based if: (i) the identity was established by means of e-identification and e-transaction trust services; or (ii) the document is available to the obliged entity in a national electronic database for five years after the end of the business relationship. The obliged entity must be capable of showing at all times during the data retention period that they have verified

or the beneficial owner has close personal and professional links with that country.

- the data obtained in the course of identification and indicate the reliable and independent source of the data and the origin of the two sources in appropriate cases;
- 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 the Guidelines, including the documents collected for compliance with the requirements set out in point 4.3 of the Guidelines;
 - 5.1.6. transaction date or period and a description of the substance of the transaction;
 - 5.1.7. information about all actions taken on a transaction or to identify the beneficial owner of the customer. If the obliged entity establishes a business relationship with a customer whose beneficial owner information must, under the law of a Member State of the European Union, be submitted to or registered in that country, the obliged entity must register and retain the appropriate certificate of registration or an extract from the register;
 - 5.1.8. upon making transactions with the representative of a civil law partnership, community or another legal arrangement or with a trust or trustee, the fact that the person has such a status. Also an extract of the registry card from the register or a certificate from the registrar of the register in which the association of persons without the status of a legal entity has been registered;
 - 5.1.9. also the following data in relation to transactions:
 - 5.1.9.1. upon opening an account, the account type, number, currency and significant characteristics of the securities or other property;
 - 5.1.9.2. 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;
 - 5.1.9.3. 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;
 - 5.1.9.4. upon entry into insurance contracts, the account number debited to the extent of the first insurance premium;
 - 5.1.9.5. upon making a disbursement under an insurance contract, the account number that was credited to the extent of the disbursement amount;
 - 5.1.9.6. 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;
 - 5.1.9.7. in the case of another transaction, the amount and currency of the transaction and the account number;
 - 5.1.10. data and documents collected in the course of monitoring the business relationship, including the documents collected for compliance with the requirements of point 4.4 of the 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);
 - 5.1.11. all of the correspondence related to the performance of the obligations arising from these Guidelines and the MLTFPA;
 - 5.1.12. the information that serves as a basis for the obligation to report to the FIU;

- 5.1.13. data of suspicious or unusual transactions or circumstances of which the Financial Intelligence Unit was not notified;
- 5.1.14. information about the circumstances of termination of the business relationship within the meaning of point 6.3.3 of the Guidelines because the application of due diligence measures is impossible.
- 5.2. The data arising from point 5.1 (excluding point 5.1.12) of the Guidelines must be retained for five (5) years after the expiry of the business relationship or the conclusion of a transaction. The data related to the performance of the reporting obligation arising from point 5.1.12 must be retained for at least five (5) 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 (5) years after the expiry of the business relationship or the conclusion of the transaction.
- 5.4. The obliged entity deletes the retained data after the expiry of the time limits, unless the legislation regulating this 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 (5) years after the expiry of the first time limit.
- 5.5. Documents and data must be retained in a manner that allows for exhaustive and immediate response to the queries made by the FIU or, pursuant to legislation, other supervision 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 (5) 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. 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 connect them with the concluded transactions quickly and understandably (if necessary, give the documents titles and retain them chronologically).

6. Refusal to establish a business relationship and conclude a transaction and (extraordinary) cancellation of a business relationship

6.1. Refusal to establish a business relationship or conclude a transaction

- 6.1.1. The obliged entity is prohibited to establish a business relationship or enable the conclusion or completion of a transaction occasionally or within the scope of a business relation if:
 - 6.1.1.1. it suspects money laundering or terrorist financing, or it cannot comply with the due diligence measures required on the basis of the MLTFPA. For example, if the customer does not submit or refuses to submit the necessary information or document or the submitted information or documents do not provide a basis for the conviction that the collected data are sufficient;
 - 6.1.1.2. the capital of the person who wants to establish a business relationship or conclude a transaction consists of bearer shares or other bearer securities to the extent of more than 10 per cent;

- 6.1.1.3. the person who wants to establish a business relationship or conclude a transaction is 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;
 - 6.1.1.4. this would require the opening of an anonymous account or savings book. Also the opening of an account clearly in the name of the wrong person;
 - 6.1.1.5. a natural person behind whom is another beneficial owner, wants to establish a business relationship or conclude a transaction (suspicion that a front is used).
 - 6.1.2. The obligation arising from point 6.1.1 of the Guidelines is not performed if the obliged entity has informed the FIU about the establishment of the business relationship, the transaction or the attempt to conclude a transaction pursuant to the procedure stipulated in point 7 of the Guidelines and/or received a specific instruction from the FIU to continue establishing the specific business relationship or concluding the transaction.
 - 6.1.3. In the case of a refusal to establish a business relationship or conclude a transaction, the obliged entity must comply with the reporting obligation in accordance with the requirements of point 7 of the Guidelines. Thereby registers and retains the details of the refusal to establish a business relationship and conclude a transaction as well as compliance with the reporting obligation in accordance with point 5 of the Guidelines.
 - 6.1.4. If the obliged entity constantly refuses to establish a business relationship or conclude transactions on the basis of point 6.1.1 of the Guidelines or if the above is refused before the application of due diligence measures, the obliged entity must carry out periodical analyses to identify:
 - 6.1.1.6. the employees or other contractual partners who primarily bring in the customers with whom it is decided to refuse to establish a business relationship or conclude a transaction;
 - 6.1.1.7. the agency, representation or other person who brings in the customers with whom it is decided not to establish a business relationship or conclude a transaction.
- 6.2. Postponement of a transaction**
- 6.2.1. The obliged entity has the right to postpone the conclusion of a transaction until the person participating in the transaction or the customer has submitted the necessary documents and information for the application of due diligence measures, including for the verification of the origin of the assets serving as the object of the transaction or for the monitoring of the business relationship.
 - 6.2.2. The obliged entity may conclude the transaction and not exercise the right specified in point 6.2.1 only if not concluding the transaction is impossible or may obstruct the efforts made to catch the persons benefiting for the suspicious transaction. The obliged entity cooperates with the FIU and complies with the reporting obligation within the meaning of point 7 of the Guidelines.
 - 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 the Guidelines that transactions may only be concluded under exceptional circumstances applies at the same time.
 - 6.2.4. If the obliged entity has not managed to apply adequate due diligence measures in the course of

the activity specified in point 6.2.3 of the Guidelines within a reasonable time in order to exhaustively collect data, make sure that the data are true or eliminate suspicion of money laundering or terrorist financing, the obliged entity must cancel the business relationship extraordinarily according to the requirements set forth in point 6.3.3 of the Guidelines.

6.3. (Extraordinary) cancellation of a business relationship

- 6.3.1. The obliged entity has the right to cancel the contract serving as a basis for a business relationship ordinarily or extraordinarily. In the case specified in point 6.3.2 of the Guidelines, the extraordinary cancellation is to be decided by the obliged entity themselves and in the case specified in point 6.3.3, the contract that serves as the basis of the business relationship must be cancelled extraordinarily without notice.
- 6.3.2. The obliged entity has the right to cancel the long-term contract serving as a basis for a business relationship extraordinarily and without notice in the case of refusal to issue the person's e-resident digital identity card, its validity is suspended or it is declared invalid on the ground stipulated in subsections 20⁶ (2) or (3) of the Identity Documents Act.
- 6.3.3. The obliged entity is obliged to cancel the long-term contract serving as the basis for the business relationship extraordinarily and without notice if there is a business relationship with the customer in a situation specified in point 6.1.1 of the Guidelines and the customer refuses to provide the information or documents required for the application of due diligence measures. This is considered a material breach of contract. The business relationship is considered terminated by giving the notice of cancellation to the customer, after which the obliged party will make the service completely unavailable to the customer²²⁶.
- 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 the Guidelines, the obliged entity will transfer the customer's assets within a reasonable time but preferably not later than within one month²²⁷ after the termination of the business relationship to an account opened in a credit institution entered in the Business 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 Council²²⁸ are applied. In exceptional cases, assets may be transferred to another account that meets the conditions listed in the previous sentence but is not the customer's account by informing the FIU about this with all the relevant and sufficient information²²⁹ at least seven (7) working days in advance and on the condition that the FIU has not issued a precept to suspend the transaction or establish a restraint on the account, the assets in the account or the assets that are the object, or in respect of other assets under suspicion of money laundering or terrorist financing. 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 obliged entity may continue with the business relationship and not exercise the right specified in point 6.3.2 of the Guidelines only if terminating the business relationship may obstruct the efforts made to catch the persons benefiting from the suspicious transaction. In such a case, the obliged entity must cooperate with the FIU by informing the FIU immediately after the conclusion

²²⁶ The scope of the obligation to justify the refusal to open or the closure of a payment account with basic features on the basis of the prevention of money laundering and terrorist financing is described in detail in points 3.11 to 3.14 of the FSA's advisory guidelines 'Requirements for providers of basic payment services' referred to in footnote 26.

²²⁷ The obliged entity takes reasonable steps to do this within one (1) month or as soon as possible.

²²⁸ See footnote 102 for the relevant directive of the European Parliament and of the Council.

²²⁹ Including 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.

of the transaction or decision to continue the business relationship.

- 6.3.6. The obliged entity may continue with the business relationship and not comply with the obligation specified in point 6.3.3 of the Guideline if the obliged entity has informed the FIU about the establishment of the business relationship, the transaction or the attempted transaction pursuant to the procedure stipulated in point 7 of the Guidelines and received a specific instruction from the FIU to continue with the business relationship. Also if the obliged entity has received an instruction from the FIU without making the prior relevant report.
- 6.3.7. In respect of the circumstances of the extraordinary termination of a business relationship, the obliged entity complies with the reporting obligation to the FIU in accordance with the requirements of point 7 of the Guidelines. The obliged entity thereby registers and retains the details of the extraordinary termination of a business relationship and the compliance with the reporting obligation in accordance with point 5 of the Guideline.
- 6.3.8. If the obliged entity constantly terminates business relationships extraordinarily on the basis of point 6.3.3 of the Guidelines, the obliged entity must prepare periodical analyses to identify:
- 6.3.8.1. the employees or other contractual partners 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;
 - 6.3.8.2. the agency, representation or other person 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;
 - 6.3.8.3. the employees that manage the customers with whom business relationships are most often terminated and for which reasons and whether such persons have failed to perform their duties or have performed them inadequately;
 - 6.3.8.4. whether it was 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.

7. Obligation to report to the Financial Intelligence Unit

- 7.1. The obliged entity must report to the FIU on (i) the activity or (ii) the circumstances that they identify in the course of economic activities and whereby:
- 7.1.1. its characteristics indicate the use of criminal proceeds or the commission of crimes related to this (this is primarily a notice about a suspicious and unusual transaction or activity, i.e. UTR²³⁰ or UAR²³¹);
 - 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 suspicious transaction report, i.e. STR²³²);
 - 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

²³⁰ In English – Unusual Transaction Report.

²³¹ In English – Unusual Activity Report.

²³² In English – Suspicious Transaction Report.

whereby terrorist financing is suspected, i.e. TFR²³³);

- 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 the Guidelines is present.
- 7.2. The Financial Intelligence Unit must be notified²³⁴:
 - 7.2.1. by the obliged entity also about the circumstances of refusal of establishment of a business relationship or conclusion of an occasional transaction on the basis of point 6.1.1 of the Guidelines and about the extraordinary cancellation of a business relationship on the basis of point 6.3.3 of the Guidelines (primarily an unusual transaction 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. CTR²³⁵).
 - 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 the Guidelines must be made before the conclusion of the transaction if the obliged entity suspects or knows that money laundering or terrorist financing or related crimes are being committed and if said circumstances are identified before the conclusion 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 conclusion of the transaction may also be appropriate in other cases²³⁶. If the postponement of a transaction may cause considerable damage, it is not possible to omit the transaction or it may impede the capture of a person who committed possible money laundering or terrorist financing, the transaction will be concluded and a report will be submitted to the FIU thereafter.
- 7.4. In any case (i.e. also in the situation where an activity or circumstance is identified after the conclusion of the transaction), the reporting obligation must be performed immediately but no later than two (2) 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). In order to ensure prompt compliance with the reporting obligation, due diligence measures must be applied promptly from the first indication of suspicion of money laundering or terrorist financing and there must be no undue delay or stoppage in the application of due diligence measures.²³⁷ The purpose of immediate reporting is to give the FIU the opportunity to have its own suspicions and apply its own measures, considering that terrorist financing is a process where criminal proceeds or assets used for criminal purposes, especially financial assets, can be transferred through the credit and financial institutions

²³³ In English – Terrorist Financing Report.

²³⁴ Upon compliance with the reporting obligation, the obliged entity also takes into account the relevant guidelines and instructions established by the FIU.

²³⁵ In English – Cash Transaction Report.

²³⁶ 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.

²³⁷ For example, an alert generated by the system used to monitor or screen transactions should be processed by the first line of defence for initial analysis and reviewed as soon as possible and, if necessary, forwarded to the second line of defence for further analysis.

of several countries in one (1) working day, which is why quick reporting helps trace black money more efficiently.

- 7.5. 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 the Guidelines, the reporting obligation must also be performed within the meaning of point 7.1 of the Guidelines, whereby this may also take place within the scope of the same report.
- 7.6. 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 FIU), 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 the Guidelines).
- 7.7. Upon the performance of the reporting obligation related to the payment service, the obliged entity also decides whether it would be appropriate to inform the Financial Intelligence Units of the other countries related to the payment about the payment and, if necessary, informs them 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 to prevent, detect and investigate money laundering and terrorist financing and to apply 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, (ii) the payee's payment service provider, and (iii) the intermediary payment service provider.
- 8.4. Sending the information of the payer and the payee requires sending information about the persons who actually (finally) 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 re-apply due diligence measures

- 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 implements 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 the Guidelines.

10. Implementation of the Guidelines

This version of the Guidelines is valid from 1 May 2024. The version of advisory guidelines of the FSA 'Organisational approaches and preventive measures of credit and financial institutions for prevention of money laundering and terrorist financing' established by FSA Management Board Resolution No. 1.1-7/172 of 26.11.2018 is declared invalid by the establishment of this version of the Guidelines.

Annex 1 – Phases of money laundering and Estonia-specific money laundering risks and risk indicators

Money laundering is divided into three phases:

- 1) **Placement** means the initial insertion of criminal proceeds into the financial system. In many scenarios, this is the physical movement of money received from financial or other crime to a credit or financial institution. The primary objective of placement is to gain access to the financial system while separating money or assets from their illicit source and origin.

The characteristics of the placement phase are:

- a) funds are placed in a current or payment account in cash (so-called payment service);
 - b) various insurance premiums are paid, and loans taken on the basis of loan agreements are repaid in cash, attempts are made to pay for fund units or other investment services in cash, etc.;
 - c) criminal proceeds received from fraud, embezzlement, tax crimes, etc. are in the current account at the moment the crime is committed, after which their layering starts.
- 2) **Layering** is the second phase of money laundering, where the proceeds of crime are separated from their source. This means distancing criminals from the source of the assets through seemingly legal transactions. The more complex and numerous the layers constructed by a financial or other criminal, the more difficult it is to identify the original source of funds.

The characteristics of the layering phase are:

- a) funds are transferred from one current or payment account to another or current and payment accounts are used to pay for various goods and services or to grant or repay loans;
 - b) 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);
 - c) a loan that was taken is repaid immediately or early, an insurance contract is cancelled after a short time or early, fund units are sold immediately or after a short time, purchased securities are sold immediately or a short time after their acquisition;
 - d) 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;
 - e) the funds in a current or payment account are withdrawn in cash and currency is also exchanged in the course of this activity in certain cases.
- 3) **Integration** is the final phase of the money laundering process, whereby 'laundered' funds are placed into the legitimate economy in a way that makes it appear to be legally obtained. Once the layering process is complete, the criminal who received the illegal proceeds must transform them into seemingly legal funds, which is the purpose of integration.

The characteristics of the integration phase are:

- a) funds are withdrawn from the current or payment account in cash (payment service) and integrated into the real economy;
- b) the funds in a current or payment account are converted into cash;

- c) 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;
- d) cars, real estate or other assets are purchased for the funds in the current or payment account, through which the funds are integrated into the real economy (payment service).

The financial system of Estonia may be taken advantage of in different phases of money laundering. This Annex is based on different threat assessments, typologies²³⁸, data accessible to the FSA, 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 as well as the geographic location of Estonia.

The biggest threats to Estonia are mainly 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 current or payment accounts or attempts are made to conceal their actual origin, including by the so-called mirror transactions.

Below is a list of products, services and ways through which Estonian credit and 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 the FSA (point 2.2.1 of the Guidelines). 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 related to money laundering.

Estonia-specific money laundering risks and risk indicators

Although the Know Your Customer principle 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 activity and conduct correspond to the information known to the financial institution, in order to manage the risk of money laundering, the financial institutions should in appropriate cases give particular attention to the following risks related to placement, layering and integration, and risk indicators:

1) Placement

- a) in the case of cash deposits:
 - i. the capacity 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;
 - ii. 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;
 - iii. 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 interest between the customer and the obliged entity because, in addition to the role of introducing, the third party provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;

²³⁸ Pursuant to clause 54 (1) 2) of the MLTFPA, the duties of the Financial Intelligence Unit include, among other things, strategic analysis that covers the risks, threats, trends, patterns and methods of operation of money laundering and terrorist financing. In relation to this, the Financial Intelligence Unit makes typology announcements on its website www.fiu.ee, the objective of which is to give the market guidelines for the identification of threats with the help of the described factors. The Financial Intelligence Unit issues different typologies in this way, publishing them on its website specified herein.

- iv. 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 point 2 (layering).
- b) in the case the obligations related to a financial service paid in cash:
- i. the person who performed an obligation in cash – the risks may be that a third party, including a party that has no connections to the customer, performs the financial obligation related to the financial service on behalf of the customer;
 - ii. the capacity 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;
 - iii. the wishes and actual intent and capacity 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;
 - iv. 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 interest between the customer and the obliged entity because, in addition to the role of introducing, the third party provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;
 - v. 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;
 - vi. 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);
 - vii. 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 point 2 (layering).

2) Layering

- a) in the case of payment services (transfer of funds)²³⁹:
- i. 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):
 - 1. the person is a politically exposed person;
 - 2. 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, including areas of conflict, or countries that have other important connections with the aforementioned countries;
 - 3. the person has no connection with Estonia, but they still want to receive the service in Estonia;
 - 4. 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

²³⁹ The FATF has defined the term 'shell company' (the term 'shelf company' is also used in other literature, which means a 'shell company' left waiting on a 'shelf') 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. Obligated 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 the FSA 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.

- conditions do not have to be present at the same time);
5. the person carries out large transactions, whilst the representative and beneficial owner of the customer is the same person, including 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.;
 6. the person has just been established or they have no previous economic activities, but they declare unusually large transaction turnovers or an unusual capacity;
 7. 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, including 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;
 8. the person's ownership structure is complicated and not associated with the customer's economic activities, including the customer is not able to justify the selection;
 9. the person uses nominee directors or nominee shareholders in their management or ownership structure, whether it is formal or informal²⁴⁰;
 10. the person's jurisdiction is not associated with the customer's economic activities, including the customer is not able to justify the selection;
 11. the person's registration address is not associated with the customer's economic activities, including the customer is not able to justify the selection;
 12. the person's tax residency is not associated with the customer's economic activities, including the customer is not able to justify the selection;
 13. the address of the person's place of business is located in an apartment building, is a post office box or is in any other way inappropriate for operating in the relevant volume in the relevant area of activity;
 14. the person wants to conclude large or relatively large transactions in the current or payment account, but the representatives or beneficial owners themselves do not want to establish financial relationships with the service provider;
 15. 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;
 16. the person's area of activity is basically an undetermined circle of activities or areas of activity that contradict each other or are completely different from each other;
 17. the person wants a financial service that does not correspond to their usual profile, capacity or wishes that are probably real;
 18. 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;
 19. 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);
 20. 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;
 21. the person's beneficial owner or representative has also opened many other accounts where they are the representatives or beneficial owners without adequate explanations as to why it is necessary to open so many accounts;
 22. the person uses a changing IP address (the so-called Proxy service);

²⁴⁰ For example, family members, business partners or other persons close to the beneficial owner, sometimes also called straw or front men.

- ii. 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):
1. 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;
 2. 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;
 3. transactions constantly take place between companies in the same group or between the same companies, who seem to be connected to each other;
 4. 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;
 5. 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 (including constantly) and this does not coincide with the customer's usual behaviour or capacity;
 6. the substance of the payment transactions is different than the activity declared by the customer;
 7. the customer constantly converts currencies, which may, among others, be economically harmful or have no reasonable purpose (currencies are constantly converted);
 8. the customer is not interested in transfer fees and 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;
 9. incoming larger amounts are divided into smaller amounts as transfers or small amounts are collected and passed on as one large payment;
 10. 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;
 11. incoming funds are constantly transferred in the same amount after a short period of time;
 12. the person does not make transfers for wages, utilities, taxes, etc. from the current or payment account;
 13. the person has no employees or other resources (including warehouses, offices, etc.) for the provision of services and the conclusion of the relevant transactions;
 14. 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).
 15. the transport service provider is not paid for the transport of the purchased or sold goods or the person does not have the capacity to transport goods themselves;
 16. 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;
 17. 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 document and not transport, etc.;
 18. goods are transported in a manner (including in packaging) that makes no sense;
 19. the quantities of goods do not comply with the reasonable economic purpose or capacity, including the number of freight wagons, shipping containers, etc. does not correspond to reasonable economic capacity;

20. the values of the goods or services declared by the transactions do not correspond to the actual values and they are undervalued or overvalued;
 21. 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 a cent or the exact price of an item of goods is an amount that ends with three (3) or four (4) zeros;
 22. signatures (and seals) have been copied onto the contracts that serve as a basis for the transaction, including they are under the text and are as images on the contract;
 23. the debt relationships that serve as a basis for the transactions are economically unreasonable or difficult to explain;
 24. the transactions on the current or payment account indicate that the account is used as a transit account;
 25. 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;
 26. 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);
 27. e-money is constantly purchased;
 28. 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;
 29. securities that do not circulate in the ordinary infrastructure of the securities market are purchased, sold or borrowed.
- iii. 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, including are areas of conflict, or countries that have other important connections with the aforementioned countries;
- iv. 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 interest between the customer and the obliged entity because, in addition to the role of introducing, the third party provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;
- v. the origin of the funds – the risks may be that the funds used in a transaction are criminal proceeds or of an unusual origin or there is no reasonable economic explanation about their origin;
- vi. 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, or the person transfers funds from their other account without an adequate explanation;
- vii. the actual location of the customer – the risks may be that the customer actually uses Internet bank solutions (IP address) in a country or the neighbouring countries of a country that is associated with a higher risk of terrorism, including is an area of conflict, or a country that has other important connections with the aforementioned countries;
- b) in the case of securities transactions (purchase and sale, i.e. including so-called mirror transactions):
- i. 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;
 - ii. 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;
 - iii. the manner of conclusion of transactions – the risks may be that the customer buys and sells securities (including constantly) outside the stock exchange;
 - iv. the speed of the transaction – the risks may be that the customer sells the securities immediately after buying them, including the transaction may be economically harmful;
 - v. the economic justification of the transaction – the risks may be that the customer sells securities (including 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;
 - vi. 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;
 - vii. the repetition of transactions – the risks may be that the customer repeatedly buys and sells securities without having clear strategic or economic reasons;
 - viii. 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 interest between the customer and the obliged entity because, in addition to the role of introducing, the third party provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;
 - ix. 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 point 2 (layering).
- c) in the case of the conversion of the funds in current and payment accounts into cash:
- i. the manner of conclusion of the transaction – the risks may be that cash is needed on account of the funds in the current 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;
 - ii. to the person who performs obligations – the risks may be that a third party who specifically provides CIT services comes to collect the cash on behalf of the customer;
 - iii. 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;
 - iv. 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 interest between the customer and the obliged entity because, in addition to the role of introducing, the third party provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;
 - v. 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 point 2 (layering).
- d) in the case of other financial services in general:
- i. 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, including repays a loan immediately after taking it or repays it early in an unusual manner, an insurance contract is cancelled 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 an unusually short period of time after their acquisition;
 - ii. 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 a short period of time after entry into the contract, (ii) with the aforementioned characteristic or separately, the customer transfers the contract to a third party without an obvious connection to the customer, or (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);
- iii. 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;
- iv. 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;
- v. 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);
- vi. 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;
- vii. 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 interest between the customer and the obliged entity because, in addition to the role of introducing, the third party provides to the customer legal services, accounting services, the service of establishment of a company and other legal structures, or other services;
- viii. 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 point 2 (layering).

3) Integration

- a) in the case of cash payouts:
 - i. a. the capacity 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;
 - ii. b. the person who received funds in cash – the risks may be that a third party, including 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;
 - iii. 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);
 - iv. 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;
 - v. 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 point 2 (layering);
 - vi. e. any other relevant risks specified in point 2 (layering) (especially risks arising from the person of the customer).
- b) in the case of purchases of goods for the funds in the current and payment account, all relevant risks specified in point 2 (layering) (especially risks arising from the person of the customer):

Annex 2 – Stages and risk indicators of terrorist financing

Terrorist financing is divided into three phases:

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.

This Annex is based on different threat assessments, typologies, data accessible to the FSA, 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 as well as the geographic location of Estonia. The Estonian economy is most vulnerable to terrorist financing at the stage of movement. For example, money collected for people in need may be transferred to a high-risk country, where there is no further control over its use.

According to the National Risk Assessment (NRA) of 2021, the level of risk of terrorist financing in Estonia is low in most sectors, medium in the financial sector and high in the area of virtual currencies. The state's vulnerability is higher than average in the non-profit sector among religious associations and charities as well as in the financial technology sector among crowdfunding service providers.

Below is a list of products, services and ways through which Estonian credit and 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 the FSA (point 2.2.1 of the Guidelines). 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 risks related to terrorist financing.

1. Fundraising

Based on various threat assessments, typologies, the data accessible to the FSA, statistics, the observations made during on-site inspections and special information and considering the risks specific to Estonia, this phase of terrorist financing may be the following in the case of Estonian financial institutions:

- (i) a customer (including a customer that is a non-profit organisation or a foundation) raises funds (including through a crowdfunding platform) in support of violent extremism and/or terrorist activities.

Although the Know Your Customer principle 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 activity and conduct correspond 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 fact that a region of operations is associated with countries with a higher terrorist financing risk ('high-risk countries')²⁴¹, including conflict zones;
 - b. the objective for which funds are raised by the non-profit association and foundation – the risks may be related to the fact that funds or other assets are raised for a person or organisation that supports or carries out violent extremism and/or terrorist activities;
 - c. the objectives of the non-profit association and foundation in general – the risks may be related to the fact that funds or other assets are raised for persons, groups, organisations, etc. that raise funds or other assets for persons, groups, organisations that in one way or another are related to countries with a higher risk of terrorist financing ('high-risk countries'), including conflict zones;
 - d. the pattern and volume of the transactions of the non-profit association, foundation or other association are not in line with the area of activity of the non-profit association, foundation or other association or the number of its employees and/or members;
 - e. cash deposits or withdrawals – the risks may be that a non-profit association or foundation constantly or once deposits cash in a current or payment account or withdraws it whilst such activity does not correspond to the activities expected from the non-profit association or foundation;
 - f. the other relevant risks highlighted under transfers made from current and payment accounts in point 2 (movement), including 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. the nature of transactions refers to the pooling and transfer of funds from different sources but does not relate to the sale of goods or the provision of services;
 - c. all circumstances with the relevant differences arising from the person, which are highlighted in point 1 (fundraising) under the services provided to non-profit associations and foundations.

2. Movement

Based on various threat assessments, typologies, the data accessible to the FSA, statistics, the observations made during on-site inspections and special information and considering the risks specific to Estonia, this phase of terrorist financing may be the following in the case of Estonian financial institutions:

- (i) the person (including a non-profit association or foundation) transfers funds to a person or organisation that supports or carries out violent extremism and/or terrorist activities. The funds may be transferred to a country with a higher risk of terrorist financing ('high-risk country') where there is no clear overview of their use.

²⁴¹ In respect of countries with higher terrorist financing risk or 'high-risk countries', see the annex to the FIU guidelines on characteristics of suspicious transactions, which addresses countries where the risk of terrorist financing is higher, both here and elsewhere in the context of this Annex 2.

Although the Know Your Customer principle 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 activity and conduct correspond 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 current 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 has or appears to have links with countries with a higher risk of terrorist financing ('high-risk countries'), including conflict zones;
 - ii. the person has no adequate connection with Estonia, but they still want to receive the service in Estonia;
 - iii. 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);
 - iv. the person carries out incomprehensible transactions, whilst the representative and beneficial owner of the customer is the same person, including 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.;
 - v. the person has just been established or has no previous economic activities, but they declare unusual transaction turnovers or an unusual capacity, i.e. the nature of the transaction does not correspond to the person's economic activities;
 - vi. the person's transaction turnovers are unusual and do not correspond to the customer's (representative's and beneficial owner's) experience, age and capacity to conclude such transactions, including the number of employees, and the main transaction partners give no reason to believe that the customer has the capacity for such transaction volumes;
 - vii. the person's ownership structure is complicated and not associated with the customer's economic activities, including the customer is not able to justify the selection;
 - viii. the person's jurisdiction is not associated with the customer's economic activities, including the customer is not able to justify the selection;
 - ix. the person's registered address is not associated with the customer's economic activities, including the customer is not able to justify the selection;
 - x. the person's tax residency is not associated with the customer's economic activities, including the customer is not able to justify the selection;

- xi. the address of the person's place of business is located in an apartment building, is a post office box or is in any other way inappropriate for operating in the relevant volume in the relevant area of activity;
 - xii. 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;
 - xiii. the person's area of activity is basically an undetermined circle of activities or areas of activity that contradict each other or are completely different from each other;
 - xiv. the person wants a financial service that does not correspond to their usual profile, capacity or wishes that are probably real;
 - xv. there is no relevant or reliable information about or trace of the person on the Internet, although they should exist considering the volume of their planned transactions and area of activity;
 - xvi. 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);
 - xvii. 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;
 - xviii. the person's beneficial owner or representative has also opened many other accounts where they are the representatives or beneficial owners without adequate explanations as to why it is necessary to open so many accounts;
 - xix. the person uses a changing IP address (the so-called Proxy service);
 - xx. the transaction and/or action is supervised by an unauthorised person;
 - xxi. the person's awareness of the transaction counterparty is insufficient;
 - xxii. the pattern and volume of the transactions of the non-profit association, foundation or other association are not in line with the area of activity of the non-profit association, foundation or other association or the number of its employees and/or members.
- b. to countries related to payments – this is probably the most important indicator and may be related to the fact that the customers of a financial institution receive or transfer funds from/to countries with a higher risk of terrorist financing ('high-risk countries'), including conflict zones;
- c. the origin of funds – risks may arise if the origin of a person's assets is unclear, the explanation is unclear or the assets are potentially of criminal origin;
- 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 with a higher risk of terrorist financing ('high-risk countries'), including conflict zones, 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 another unusual kind of aid;

- e. payment details – the details of the transaction may refer to violent extremist ideology or support for terrorism or a donation handout or may not be translatable or understandable. The details of the transaction are not in line with the person’s general economic activities or usual practices;
 - 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 from or their place of residence or business is in a country with a higher risk of terrorist financing (‘high-risk country’), including in a conflict zone;
 - h. the actual location of the customer – the risks may be related to the fact that the customer actually uses Internet bank solutions (IP address) in countries related to a higher risk of terrorist financing (‘high-risk country’), including in conflict zones;
 - i. the activities of the customer – the risks may be related to the fact that the customer or the persons related to them have a connection to countries with a higher risk of terrorist financing (‘high-risk country’), including conflict zones, which may constitute the sale or purchase of products and services to or from such countries;
 - j. the customer’s counterparty risk – the risks may be related to the fact that the customer’s transaction partner is associated with countries with a higher terrorist financing risk (‘high-risk countries’), including conflict zones. For example, it is a credit or financial institution that is registered or provides services in a high-risk country (such as a payment institution, payment agent) or is known to be a user of a virtual IBAN account;
 - k. the other activities of the customer – the risks may be related to the fact that the other activities and initiatives of the customer or the persons associated with them (representatives, beneficial owners, etc.) are connected to countries with a higher risk of terrorist financing (‘high-risk country’), including conflict zones;
 - l. the currency used – the risks may be related to the fact that currencies are used in transactions used in countries with a higher risk of terrorist financing (‘high-risk country’), including conflict zones;
 - 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 interest between the customer and the obliged entity because, in addition to the role of introducing, the third party 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, including to a person to whom the customer is not connected;

- b. the other relevant risks highlighted under transfers made from current and payment accounts in point 2 (movement).

3. Use of funds

Based on various threat assessments, typologies, the data accessible to the FSA, statistics, the observations made during on-site inspections and special information and considering the risks specific to Estonia, this phase of terrorist financing may be the following in the case of Estonian financial institutions:

- (i) the customer withdraws funds from a current 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 another unusual kind of aid.

Although the Know Your Customer principle 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 activity and conduct correspond 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 current and payment accounts:
 - a. the place where cash is withdrawn – the risks may be related to the fact that the customer withdraws cash in the countries or the neighbouring countries of the countries related to a higher risk of terrorist financing ('high-risk country'), including conflict zones;
 - 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. withdrawal of the amount in an account – the risks may be related to the fact that the customer withdraws all or most of the money in a current account in cash;
 - d. the other relevant risks highlighted under transfers made from current and payment accounts in point 2 (movement);
2. in the case of transfers made from current 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 another unusual kind of aid;
 - b. the person sends all or most of the money in the account to connected persons;
 - c. the other relevant risks highlighted under transfers made from current and payment accounts in point 2 (movement), including the risk arising from the person of the customer.

Comprehensive obligation

In order to prevent terrorist financing, Estonian financial institutions (the obliged entities specified in point 2.2.1 of the Guidelines) must consider, in the case of all of the above, the implementation of 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 sanction, or (ii) an attempt is made to transfer funds to such a person or to make the funds accessible in any other manner.