FINANTSINSPEKTSIOON

‘Measures for the Prevention of Money Laundering and Terrorist Financing in Credit Institutions and Financial Institutions’
Advisory Guidelines of the Financial Supervision Authority

These guidelines were approved by Decision no. 1.1-7/46 of the Management Board of the Financial Supervision Authority of 3 July 2013.

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

Table of Contents

1. Jurisdiction

1.1. Under § 3 of the Financial Supervision Authority Act (hereinafter the FSA Act), in order to enhance the stability, reliability, transparency and efficiency of the financial sector, to reduce systemic risks and to promote prevention of the abuse of the financial sector for criminal purposes, with a view to protecting the interests of clients and investors by safeguarding their financial resources, and thereby supporting the stability of the Estonian monetary system.

1.2. Under subsection 2 of § 47 of the Money Laundering and Terrorist Financing Prevention Act (hereinafter the AML/CFT Act), the Financial Supervision Authority exercises supervision over fulfilment by credit institutions and financial institutions which are subject to supervision by the Financial Supervision Authority under the FSA Act of the requirements arising from this Act and legislation adopted on the basis thereof. The Financial Supervision Authority shall exercise supervision pursuant to the procedure provided for in the FSA Act.

1.3. Under subsection 1 of § 57 of the FSA Act, the Financial Supervision Authority has the right to issue advisory guidelines to explain legislation regulating the activities of the financial sector and to provide guidance to subjects of financial supervision.

2. Purpose and scope

2.1. Purpose

2.1.1. The purpose of this Guidelines (hereinafter the Guidelines) is to provide credit institutions and financial institutions with advisory clarifying instructions for the application of the requirements of the AML/CFT Act, which is aimed at the prevention of the exploitation of the financial sector for criminal purposes, avoidance of systemic risks and, thus, increasing the stability, reliability and transparency of the sector.

2.1.2. These advisory Guidelines explain the requirements established in the AML/CFT Act, which are aimed at the obligated persons. The Guidelines cover the requirements for assessment and management of the risk of money laundering and terrorist financing and the rules of procedure thereof, including establishment of business relationships, surveillance of transactions, internal audit rules for auditing customer due diligence and actions required in the event of suspicion of money laundering (performance of the reporting obligation).

2.2. Scope of application

2.2.1. The Guidelines are aimed at credit institutions and financial institutions that provide services in the Republic of Estonia and are obligated persons for the purposes of the requirements established in the AML/CFT Act and subject to supervision by the Estonian Financial Supervision Authority,[1] i.e. credit institutions, life insurance companies and life insurance brokers, management companies and investment funds established as public limited companies, investment undertakings, payment institutions and e-money institutions as well as credit institutions and financial institutions of listed foreign countries which provide cross-border services in Estonia, and branches of foreign credit institutions and financial institutions registered in the commercial register of the Republic of Estonia (hereinafter obligated persons).

2.2.2. Upon application of these Guidelines, the requirements arising from the legislation in force and from other advisory guidelines of the Estonian Financial Supervision Authority must be taken

[1] The subjects of supervision of the Estonian Financial Supervision Authority are specified in the FSA Act.

into account. In the event of imperative requirements arising from legislation, the provisions of legislation must be followed. If application and interpretation problems arise upon application of the Guidelines, the principle of reasonableness must be followed in light of the purpose of these Guidelines and the principle of good faith must be upheld in accordance with the duty of customer due diligence expected of an obligated person.

2.2.3. In such circumstances, the "comply or explain" principle must be followed. According to the principle, a data subject must be able to explain, where necessary, why it does not adhere to certain articles of the Guidelines or only adheres to them in part.

3. Underlying principles

3.1. Money laundering means concealment or maintenance of the confidentiality of the true nature, origin, location, manner of disposal, relocation or right of ownership or other property-related rights acquired as a result of a criminal activity or property acquired instead of such property as well as conversion, transfer, acquisition, possession or use of property acquired as a result of a criminal activity or property acquired instead of such property with the purpose of concealing the illicit origin of the property or assisting a person who participated in the criminal activity so that the person could escape the legal consequences of their actions.

3.2. Terrorist financing means a situation where a person wilfully and directly or indirectly transmits or gathers assets[2] with the illegal intent to directly or indirectly support the committing of a terrorist act,[3] a terrorist organisation or an individual terrorist. Terrorist financing is not limited to a situation where funds have actually been used to commit a terrorist act or an attempt thereof or a situation where terrorist financing can be directly associated with a terrorist act.

3.3. Upon prevention of terrorist financing it must be made certain, among other things, that persons are not directly engaged in or indirectly support the financing of proliferation[4] by attracting funds, i.e. the making, acquisition, development, export, reloading, mediation, carriage, warehousing or use of nuclear, chemical or biological weapons or other materials meant for making such weapons.[5]

4. General requirements

4.1. Customer due diligence

4.1.1. Customer due diligence is one of the main tools for ensuring the implementation of legislation aimed at preventing money laundering and terrorist financing and at applying sound business practices. Customer due diligence comprises a set of activities and practices arising from the organisational and functional structure of an obligated person and described in internal

---

[2] Thereby it is irrelevant whether the assets are of legal or illegal origin.

[3] Under subsection 1 of § 237 of the Penal Code, a terrorist act means the committing of a criminal offence against international security, against the person or against the environment, against foreign states or international organisations or a criminal offence dangerous to the public posing a threat to life or health, or the manufacture, distribution or use of prohibited weapons, the illegal seizure, damaging or destruction of property to a significant extent or interference with computer data or hindrance of operation of computer systems as well as threatening to carry out such acts, if committed with the purpose of forcing the state or an international organisation to perform an act or omission, or to seriously interfere with or destroy the political, constitutional, economic or social structure of the state, or to seriously interfere with or destroy the operations of an international organisation, or to seriously terrorise the population.

[4] For further information on financing of proliferation see FATF Recommendation 7. See also the website of the Estonian Internal Security Service available at http://www.kapo.ee/est/toovaldkonnad/terrorism/massihavitusrelvad. (05.06.2013).

[5] For further information see UN Security Council Resolutions 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010).

procedures, which have been approved by the directing bodies of the obligated person and the implementation of which is subject to control systems established and applied by internal control rules.

4.1.2. The purpose of customer due diligence is to prevent the use of assets and property obtained in a criminal manner in the economic activities of credit institutions and financial institutions and in the services provided by them whose goal is to prevent the exploitation of the financial system and economic space of the Republic of Estonia for money laundering and terrorist financing. Customer due diligence is aimed, first and foremost, at applying the *Know-Your-Customer* principle,[6] under which a customer must be identified and the appropriateness of transactions must be assessed based on the customer's principal business and prior pattern of payments. In addition, customer due diligence serves to identify unusual circumstances in the operations of a customer or circumstances whereby an employee of the obligated person has reason to suspect money laundering or terrorist financing.

4.1.3. Customer due diligence must ensure the application of adequate risk management measures in order to ensure constant monitoring of customers and their transactions and the gathering and analysis of relevant information. Upon applying the customer due diligence measures, the obligated person may follow the principles compatible with its business strategy and, based on prior risk analysis[7] and depending on the nature of the customer's business relationships, apply customer due diligence to a different extent.

4.1.4. Customer due diligence must be applied based on risk sensitive basis, i.e. the nature of the business relationship or transaction and the risks arising therefrom must be taken into account upon selection and application of the measures. Risk-based customer due diligence calls for the prior weighing of the specific business relationships or transaction risks and, as a result thereof, qualification of the business relationship in order to decide on the nature of the measure to be taken (for instance, normal, enhanced or simplified due diligence measures could be applied).

4.1.5. If the risk level of a customer or a person participating in a transaction is low, the obligated person may apply simplified due diligence measures, but is not allowed to skip customer due diligence entirely. If the risk level arising from a customer or a person participating in a transaction is high, enhanced due diligence measures must be applied.

4.1.6. Upon establishing a business relationship, the obligated person must identify the person and verify their right of representation based on reliable sources, identify the beneficial owner and, in the case of companies, the control structure, as well as identify the nature and purpose of possible transactions, including, if necessary, the source and origin of the funds involved in the transactions.

4.1.7. Customer due diligence also involves the obligated person's duty to identify and know the customer's economic transactions, thereby the obligated person must constantly assess the substance and purpose of the customer's transactions and operations with the level of diligence expected of a credit institution or financial institution, in order to identify the possible relations of the transaction or the funds used with money laundering or terrorist financing. Ongoing review consists of monitoring the transactions executed in the course of the business relationship so that the obligated person may understand the purpose of the business relationship established with the customer, the nature of the business operations of the customer, and, if needed, know the source and origin of the funds used in the transactions.

4.1.8. Customer due diligence measures are appropriate and with suitable scope if they make it possible to identify transactions aimed at money laundering and terrorist financing and identify

[6] Know-Your-Customer (KYC).
[7] See section 4.6 of these Guidelines.

suspicious and unusual transactions as well as transactions that do not have a reasonable financial purpose or if they at least contribute to the attainment of these goals.

4.1.9. The first requirement for the measures of prevention of money laundering and terrorist financing is that the obligated person does not enter into transactions or establish relationships with anonymous or unidentified persons. Legislation requires that obligated person waive a transaction or the establishment of a business relationship if a person fails to provide sufficient information to identify the person or about the purpose of the transactions or if the operations of the person involve a higher risk of money laundering or terrorist financing. Also, legislation requires obligated persons to terminate a continuing contract without the advance notification term if the person fails to submit sufficient information for application of customer due diligence measures.

4.1.10. An obligated person must ensure that information concerning a customer (incl. gathered documents and details) are up to date. In the event of customers or business relationships falling in the high risk category, the existing information must be verified more frequently than in the event of other customers/business relationships. The respective data must be preserved in writing or in a form that can be reproduced in writing and made available to all relevant employees who need it to perform their employment duties (e.g. management board members, account managers, risk managers and internal auditors).

4.1.11. The principles and instructions provided for in the customer due diligence measures must be set out in the internal procedures of the obligated person. Independent control mechanisms must be established over adherence to these procedures and the relevant training of employees must be ensured.

4.2. Organisation structure

4.2.1. To follow the Guidelines, the organisational structure, area of responsibility and knowledge and skills of the executives of credit institutions and financial institutions and the activities based thereon must comply with legislation.

4.2.2. The management board[8] of an obligated person must regularly review the efficiency of the internal procedures implemented for the purpose of complying with the AML/CFT Act and these Guidelines and ensure internal control over following the internal procedures. The obligated person appoints the person(s) who is (are) responsible at the management board level for the application of the customer due diligence measures provided for in the AML/CFT Act. The competence and responsibilities of the person must transparently and unambiguously arise from internal documentation regulating the tasks and functions of the members of the management board (e.g. rules of procedure of the management board, job descriptions of the members of the management board and service contracts of the members of the management board).

4.2.3. The person(s) appointed by the management board of the obligated person must ensure the application of customer due diligence measures based on the provisions in legislation and these Guidelines and take into account that the measures applied are adequate, correspond to the operating profile of the service provider and comply with the customer, nature and scope of the transactions and the related risks of money laundering or terrorist financing.

4.2.4. The management board of the obligated person ensures that the resources allocated to comply with the AML/CFT Act and these Guidelines are sufficient and that the employees directly

[8] The management board or 'senior management'; in the case of branches, the said person is the chief executive officer of the branch.

involved in the fulfilment of the requirements of the AML/CFT Act are fully aware of the requirements of the AML/CFT Act and these Guidelines.

4.2.5. Each executive and employee directly involved in the implementation of the AML/CFT Act and these Guidelines must have professional skills that allow them to fully and with sufficient accuracy adhere to the provisions of legislation and these Guidelines in accordance with the scope of their responsibilities and they must have completed the respective training or been otherwise instructed therein by the obligated person.

4.2.6. The obligated person mitigates and prevents conflicts of interests with internal rules, whereby the grounds of remuneration of executives and employees encourage them to disregard or deviate from provisions of law and the Guidelines.

4.2.7. Customer due diligence is part of the overall risk management framework where a clear distinction must be made between the application of customer due diligence measures applied in business relationships and the application of measures for prevention of money laundering and terrorist financing in the obligated person's own operations.

4.2.8. The obligated person must provide contractual partners (in the event of outsourcing) and all relevant staff, including staff whose duties include the establishment of business relationships and/or the execution of transactions, management of customer relationships, with regular training[9] in and notification[10] about the nature of the risks of money laundering and terrorist financing and any new trends in the field. First and foremost, staff must be kept informed about the requirements governing the prevention of money laundering and terrorist financing with respect to the application of customer due diligence measures and reporting on suspected money laundering.

4.2.9. The obligated person must ensure that the customer due diligence measures and data collection and preservation requirements applied in its third-country representations, branches or majority-held subsidiaries[11] comply with the AML/CFT Act and the requirements set out in these Guidelines. In a situation where it is not possible to fulfil such requirements due to the specific nature of local laws, the Estonian Financial Supervision Authority must be notified thereof immediately.

4.3. Economic or professional activities via agents and outsourcing[12]

4.3.1. An obligated person has the right, taking account the special requirements and restrictions provided by law, to use the services of a third party under a contract the subject of which is the continuing performance of activities and continued taking of steps required for the provision of (a) service(s) by obligated persons to their customers and that would normally be performed and taken by the obligated person itself. For the purposes of this section, third parties include, for instance, agents, subcontractors and other persons to whom the obligated person transfers the activities relating to the provision of the services provided as a rule by the obligated person in its economic activities.

4.3.2. The obligated person must choose the third party specified in the previous section with customer due diligence, in order to ensure the ability of the person to fulfil the requirements

[9] In the event of new employees, before they commence work.
[10] At least once a year.
[11] Representations, branches and majority-held subsidiaries are obligated persons for the purposes of the AML/CFT Act.
[12] The 'Requirements for Outsourcing by Subject of Financial Supervision Subject' guidelines contain more detailed requirements for obligated persons on how to ensure the transfer of one's activities to third parties in accordance with the requirements of subsection 2 of § 28 of the AML/CFT Act.

provided for in the AML/CFT Act and these Guidelines and to ensure the reliability and the required qualifications of such a person.

4.3.3. The third party specified in section 4.3.1 of these Guidelines is subject to all of the requirements provided by law for prevention of money laundering and terrorist financing regarding outsourced activities. The obligated person who outsourced its activities is liable for infringement of the requirements.

4.3.4. Upon outsourcing an activity (activities), the obligated person must ensure that the third party has the knowledge and skills required, above all, for the identification of situations of a suspicious and unusual nature and is able to meet all of the requirements for the prevention of money laundering and terrorist financing provided by law. To comply with the provisions in this section, the obligated person must ensure the notification of the executives of the third party of the relevant requirements and the training of its staff in the prevention of money laundering and terrorist financing to the extent described in section 4.2.8.

4.3.5. Upon outsourcing an activity to third parties, the obligated person must ensure that any documents and information collected for the fulfilment of requirements arising from legislation are preserved in accordance with the procedure established in the AML/CFT Act and any legislation issued on the basis thereof. The contract must ensure that relevant information is handed over to the obligated person and that the relevant information and documents are archived in accordance with its rules of procedure.

4.3.6. The outsourcing contract must specify the rights and duties of the obligated person upon reviewing compliance by the third party with the requirements provided by law. The outsourcing of economic activities to a third party must not impede state supervision over the obligated person and the latter must, under contract, grant the Financial Supervision Authority access to the third party for supervisory purposes to whom the obligated person has outsourced its duties, tasks or functions.

4.3.7. Whilst services are provided by third parties, situations where the application of customer due diligence measures to the required extent is possible to an insufficient degree or entirely impossible must be avoided. A third party must be able to fully apply the required customer due diligence measures, thereby being able to notify the contact person of the obligated person immediately and to decline a transaction. The obligated person must, under contract, ensure its right to terminate the contract with the third party if the latter fails to perform its contractual duties or obligations or performs the unduly.

4.3.8. The obligated person must immediately notify the Financial Supervision Authority of entry into a contract serving as the basis for outsourcing its activity (activities).

4.3.9. The provisions of section 4.3 of the Guidelines must be ensured by the obligated person via a contractual stipulation of the duty or obligation in the outsourcing contract.

4.4. Appointment of a compliance officer

4.4.1. The management board of the obligated person must appoint a compliance officer.[13] The functions of a compliance officer may be performed by one employee or several employees and/or a structural unit with the relevant duties. If the functions of the compliance officer are performed by a structural unit, the head of the relevant structural unit will be responsible for the performance of the functions.

[13] For further information about the requirements for appointment of a compliance officer see subsection 3 of § 29 of the AML/CFT Act.

4.4.2. The position of a compliance officer within the organisational structure of the obligated person must allow for the performance of the requirements provided by law for the prevention of money laundering and terrorist financing. Upon establishment of the compliance officer position, the compliance officer must be made directly accountable to the management board of the obligated person and made as independent of business processes as possible.

4.4.3. The compliance officer's independence from business processes does not mean that the officer is prohibited to advise or train colleagues for the purpose of ensuring the compliance of the actions of the executives and employees with the requirements of the AML/CFT Act and these Guidelines.

4.4.4. The professional qualifications and skills of the compliance officer must meet the requirements established in the AML/CFT Act and the compliance officer's professional and business reputation must be impeccable.

4.4.5. Under subsection 3 of § 31 of the AML/CFT Act, the functions of the compliance officer are as follows:

- organisation of collection and analysis of information referring to unusual transactions or transactions suspected of money laundering or terrorist financing in the activities of the obligated person (collection of information means collection of any and all suspicious or unusual notices received from the employees, contractual partners and agents of the obligated person, and systemising and analysis of the information contained in them);
- reporting to the Financial Intelligence Unit (FIU) in the event of suspicion of money laundering or terrorist financing (notice being given in the manner agreed with the FIU);
- periodic submission of written statements on implementation of the rules of procedure to the management board of the credit institution or financial institution or the head of the branch of the foreign credit institution or financial institution registered in the Estonian commercial register; and
- performance of other obligations related to the fulfilment of the requirements of the AML/CFT Act by the credit institution or financial institution (including instructing and training employees and applying respective control mechanisms).

4.4.6. The compliance officer must have access to the information forming the basis or prerequisite for establishing a business relationship, including any information, data or documents reflecting the identity and business activity of the customer. The management board also grants the compliance officer the right to participate in the meetings of the management board if the compliance officer deems this necessary to perform their functions.

4.4.7. The contact details of the compliance officer must be communicated to the Financial Supervision Authority. The compliance officer must inform the Financial Supervision Authority within a reasonable term about the appointment of a new compliance officer or a change in contact details.

4.5. Requirements for procedural rules

4.5.1. The management board of the obligated person must ensure customer due diligence in accordance with the recommendations of these Guidelines and ensure that the measures taken are appropriate, match the profile of the operations of the service provider and are in compliance with the nature and scope of the customers and transactions and the related money laundering and terrorist financing risks.

4.5.2. The rules of procedure must include instructions for updating them, describing operating procedures, applying relevant review mechanisms and respective instructing of staff.

4.5.3. The rules of procedure must include rules for the application of customer due diligence measures, assessment and management of the risk of money laundering and terrorist financing, including regular and *ad hoc* notification of the management, information collection and preservation, and the performance of the obligation to notify the FIU. The rules of procedure must describe the exact actions[14] that the obligated person performs upon establishing customer relationships and upon occasional execution and mediation of transactions for the purpose of customer due diligence.

4.5.4. The rules of procedure must contain, among other things, a procedure for identifying the customer and its activities, the beneficial owners, the source and origin of funds involved in transactions, the purpose of transactions, the counterparties of transactions, politically exposed persons or subjects of international sanctions. Likewise, the principles of preservation of respective data, following transactions in real time (*screening*) and analysing them later (*monitoring*) must be set out in the rules of procedure for the purpose of identifying and notifying of suspicious and unusual transactions.

4.5.5. In accordance with other internal control rules, the rules of procedure provide for the duties and obligations of the persons or structural units in charge of the application of customer due diligence measures, adherence to the procedure for training and notification set out in section 4.2.8 of these Guidelines, and supervision thereof. In addition to the processes relating to the application of customer due diligence measures, the procedures must ensure supervision over the application of the measures and regular assessment of the respective processes, in order to ensure the proportional effect of application mechanisms and control mechanisms along with other internal regulations.

4.5.6. The rules of procedure of obligated persons must be in writing. The rules of procedure may be included in various documents and made available to staff in a form that can be reproduced in writing.

4.5.7. Upon application of the measures described in the rules of procedure, the risk-based approach must be followed entirely and therefore the risk of money laundering and terrorist financing must be continuously assessed with regard to various actions and steps and, if necessary, the measures must be enhanced or updated.

4.6. Risk-based approach

4.6.1. The obligated person must recognise, assess and understand money laundering and terrorist financing risks in its own activities and in the activities of its customers and take measures to mitigate the risks. The applicable measures must correspond to the identified risk level.

4.6.2. In the event of the risk-based approach, the obligated person must assess the probability of the realisation of risks and what the consequences of their realisation are. Upon assessment of probability, the chance of an increase in the threat and the possibility of occurrence of the respective circumstances must be taken into account, e.g. the possible threats that may influence the activities of the customer and the service provider must be taken into account.

4.6.3. Obligated persons must take all customer due diligence measures. The scope of taking the measures depends on the characteristics of the given business relationship or the risk level of the person or customer participating in the transaction or official act; thereby the *Know-Your-Customer* principle must be followed.[15] The AML/CFT Act provides for a few exceptions to the

[14] For instance, if the rules of procedure describe how to identify a person, which data is to be verified and collected must be set out.
[15] See section 6.2 of these Guidelines.

automatic application of certain customer due diligence measures, e.g. the amount-based reporting obligation in accordance with subsection 3 of § 32 of the AML/CFT Act.

4.6.4. Upon identifying and substantiating the risk levels of a customer or a person participating in a transaction, the obligated person must take into account, among other things, the following risk categories:[16]

4.6.4.1. *Customer risk* whose factors arise from the person or customer participating in a transaction; among other things, the following must be taken into account:

- the legal form, management structure, field of activity of the person, including whether it is a trust fund, civil law partnership or another similar contractual legal entity or a legal person with bearer shares;
- whether it is a politically exposed person;[17]
- whether the person is represented by a legal person;
- whether a third party (individual) is the beneficial owner;[18]
- whether the identification of the beneficial owner is impeded by complex and non-transparent ownership relations;
- the residency of the person, including whether it is a person registered in a territories with a low tax rate;[19]
- whether the person is subject to an international sanction;[20]
- the possibility of classifying the customer as a typical customer of a certain customer category;
- circumstances (including suspicious transactions identified in the course of a prior business relationship) resulting from the experience of communicating with the person, its business partners, owners, representatives and any other such persons;
- the duration of the operations and the nature of business relationships;
- the type and characteristics of the service provided or product sold (whether the service or product is unusual or economically impracticable; whether the service or product may be related to crime or development of weapons of mass destruction; whether there is a considerable distance between the customer's seat and the destinations of the service or product; etc.);
- whether the person participates in transactions where cash plays a major role (e.g. currency exchange locations and gambling operators);
- whether the person's customers are the same or change constantly;
- whether the person's customer base has increased rapidly;
- whether the person renders the service to anonymous customers;
- the existence and nature of the risk factor relating to a service provider used to forward the service or product;
- the type and characteristics of the services used or products consumed by the person outside the obligated person;
- the nature of the personal activities of an individual;
- whether the origin of the person's assets or the source and origin of the funds used for a transaction can be easily identified; and
- whether the person has been identified face-to-face or via the Internet.

[16] Obligated persons may use other classifications of risk categories and lists of determining their factors.
[17] The meaning of the term 'politically exposed person' is given in section 7.2 of these Guidelines.
[18] See section 7.3 of these Guidelines.
[19] The list of tax-free and low-tax territories is available online at http://www.emta.ee/index.php?id=1950 (05.06.2013).
[20] Consolidated list of persons, groups and entities subject to EU financial sanctions. Available at: http://eeas.europa.eu/cfsp/sanctions/consol-list_en.htm (05.06.2013)

4.6.4.2. *Product or service risk*, whose risk factors result from the customer's economic activities or the exposure of a specific product or service to potential money laundering risks, among other things:

- private banking and personal banking;
- currency exchange and conversion transactions;
- provision of alternative means of payment and e-money;
- provision of gambling services in a casino, online and at sports events;
- purchase and sale of gold, incl. scrap gold[21] and precious stones;
- purchase and sale of high-value goods;[22]
- provision of online advertising;
- provision of innovative services; and
- foundation, sale and administration of companies.

4.6.4.3. *Country or geographical risk*, whose factors arise from differences in the legal environment of various countries:

- whether the country applies legal provisions that are in compliance with the international standards of prevention of money laundering and terrorist financing[23]; whether there is a high crime rate (incl. drug-related crime rate) in the country;
- whether the country cooperates with a criminal group; whether criminal groups use the country to pursue their operations;
- whether the country engages in proliferation;[24]
- whether there is high level of corruption in the country;
- whether international sanctions have been or are being imposed on the country;[25] and
- whether other measures[26] have been taken against or positions of international organisations[27] have been expressed on the country.

4.6.5. Taking account of the aforementioned risk categories, the obligated person must determine the risk level[28] of the person or customer participating in a transaction, e.g. whether the customer's money laundering or terrorist financing risk level is low, normal or high or whether it corresponds to other risk level qualifications determined and used by the obligated person.

4.6.6. To determine the impact of each risk category, the obligated person must assess the likelihood of occurrence of risk factors in the risk category. To determine the impact of a specific risk category, the qualifying quantity[29] of occurrence of the risk factors characterising it may be used for the purpose of deeming a specific risk factor as 'having an impact' or as 'not having an impact' in the event of exceeding a certain threshold.

---

[21] In Estonian: *romukuld.*

[22] Also, 'trading in high-value goods'.

[23] Third country equivalence list. Available at: http://ec.europa.eu/internal_market/company/docs/financial-crime/3rd-country-equivalence-list_en.pdf (05.06.2013)

[24] See section 3.3 of these Guidelines.

[25] List of restrictive measures applicable to countries. Available at: http://www.vm.ee/?q=et/taxonomy/term/89 (05.06.2013).

[26] List of high-risk and non-cooperative jurisdictions. Available at: http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/ (05.06.2013).

[27] See the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL). Available at: http://www.coe.int/t/dghl/monitoring/moneyval/default_EN.asp. (08.02.2013); Office of Foreign Assets Control. Available at: http://www.ustreas.gov/offices/enforcement/ofac/. (05.06.2013).

[28] Annex 1 contains a possible model for the assessment of risk categories and determining a customer's risk level, which takes into account the provisions of section 4.6 of the Guidelines.

[29] Upon determining the qualifying quantity and impact of each risk factor, the positions formed based on the prior experience of the obligated person must be taken into account.

4.6.7. Certain guidelines in the event of specifying a low level of risk

4.6.7.1. The customer's risk level is generally considered low if there is no risk factor of impact in any risk category and it can therefore be claimed that the customer and its operations demonstrate elements that do not differ from those of an ordinary and transparent person;[30] thereby there is no reason to suspect that the customer's operations may increase the probability of money laundering and terrorist financing.

4.6.7.2. In a situation where the application of the required measures of customer due diligence arises from legislation and information about the customer and its beneficial owner is publicly available,[31] where the operations and transactions of the person are in line with its day-to-day economic activities and do not differ from the payment conventions and conduct of other similar customers or where the transaction is subject to quantitative or other absolute restrictions, the obligated person may deem the customer's estimated money laundering or terrorist financing risk to be lower.

4.6.7.3. In a situation where at least one risk category can be qualified as high, the risk level of money laundering or terrorist financing cannot usually be low. Equally, a low risk does not necessarily mean that the customer's operations cannot be associated with money laundering or terrorist financing at all.

4.6.7.4. If the risk resulting from a business relationship, a customer or transaction is low due to risk factors established with respect to the party to the transaction or the customer and the other conditions[32] set out in § 18 of the AML/CFT Act have been fulfilled, the obligated person may apply simplified due diligence measures, but may not omit the customer due diligence measures entirely. Upon application of customer due diligence measures by way of the simplified procedure, the obligated person may determine the scope of application of the customer due diligence measures.

4.6.8. Certain guidelines in the event of specifying a high level of risk

4.6.8.1. The customer's risk level is usually high, when assessing the risk categories on the whole it seems that the customer's operations are not ordinary or transparent; there are risk factors of impact due to which it may be presumed that the likelihood of money laundering or terrorist financing is high or considerably higher. The customer's risk level is also high if a risk factor as such calls for this.[33] A high risk does not necessarily mean that the customer is laundering money or financing terrorists.

4.6.8.2. If the obligated person feels that the risk level of a customer or a person participating in a transaction is high, the obligated person must apply customer due diligence measures pursuant to the enhanced procedure[34] in order to adequately manage the respective risks. Thereby enhanced due diligence measures must be applied in accordance with § 19, 21 or 22 of the AML/CFT Act.

4.6.9. The obligated person must document the determination of the risk level, update it and make the data available to competent authorities, if necessary.

---

[30] i.e. corresponding to an average, reasonable person.

[31] For instance, publicly traded companies, state authorities and local authorities, foundations, credit institutions and financial institutions registered in the contracting states of the European Economic Area or in a third country where equivalent rules for the prevention of money laundering and terrorist financing are applied.

[32] Customer due diligence measures may only be applied by way of the simplified procedure under the conditions established in § 18 of the AML/CFT Act.

[33] For instance, situations involving a politically exposed person, a person providing services using alternative means of payment or a person subject to an international sanction. (This is not an exhaustive list and the obligated person must rely on its prior experience in identifying the respective risk factors.)

[34] Enhanced due diligence measures include duties arising from § 19 of the AML/CFT Act.

5. Establishment of business relationships

5.1. The terms of a long-term contract underlying a business relationship must also be included in the general terms and conditions of the provision of services by an obligated person and/or in the general and/or other standard terms and conditions of a settlement contract or other contracts.

5.2. The business relationships between obligated persons and customers are regulated by contracts made in writing, in a form that can be reproduced in writing or electronically.

5.3. The prerequisite for the establishment of a business relationship is an explicit and recorded certification by the customer that it will fulfil the conditions established by the obligated person for the establishment of the business relationship and execution of transactions.

5.4. The internal procedures of the obligated person must set out the terms and conditions on the basis of which the services to be used by the customer and the scope of the services will be determined. The obligated person must make certain in advance that the services provided match the substance of the actual declarations of intent by the customer, are in accordance with the nature and purposes of the given contract and correspond to the risk level attributed to the customer.

5.5. The rules of procedure regulating the establishment of a business relationship must, in addition to provisions of law, contain the following:

- the procedure for introducing the prerequisites for the establishment of a business relationship, entry into long-term contracts and execution of transactions (including the procedure for recording the customer's declaration of intent and identification of the purpose of the business relationship and the transaction) by the obligated person;
- the requirement for receiving confirmation from the customer that the customer is aware of and has understood the duties and obligations established by the relevant conditions, including the request[35] for information required for the establishment of the business relationship by and the form of submission of the information.

5.6. Upon the establishment of a business relationship, the customer or its representative and the representative of the obligated person must be in the same place.[36] This means that a potential customer or its representative has a direct contact with the representative of the obligated person. A direct contact calls for direct communication between the representative of the obligated person and the customer for the purpose of assessing the compliance of the substance of the customer's declaration of intent and purpose with the customer's true will. Thereby it is possible to specify the customer's risk level more accurately with the help of what is experienced in the course of the direct contact. The contact may occur outside the principal place of business of the obligated person if, in the course thereof, at least the same customer due diligence measures are performed as in ordinary instances.

5.7. In events provided by law and in exceptional events accepted by the management board of the obligated person or the management board of the authorised person beforehand, a business relationship may be established without a direct contact (i.e. without being in the same place as the customer), provided that the circumstances of the exceptional events have been clearly formulated in the rules of procedure of the obligated person.

5.8. The instances and procedure for the establishment of business relationships without direct contact must be provided for separately in respective procedural rules, including measures for subsequent customer due diligence measures and the management of related risks. The rules of procedure for

[35] The rules of procedure must provide for informing the customer of the liability arising from providing the wrong, misleading or insufficient information upon establishment of the business relationship and/or conducting transactions.

[36] As a rule, a business relationship cannot be established via telecommunications, but § 15 of the AML/CFT Act provides for exceptions to this rule.

the establishment of a business relationship without direct contact must set out a procedure by applying which it is possible to ensure compliance with the conditions set out in subsection 4 of § 15 of the AML/CFT Act. The rules of procedure must set out at least the following:

- a code of conduct for accepting or executing payment instructions prior to the application of all the customer due diligence measures;
- a code of conduct in a situation where identification of the person and other information is performed using electronic means of identification;
- the code of conduct for a situation where the required customer due diligence measures cannot be applied (a person cannot be identified within the prescribed time limit), as a result of which the customer's declarations of intent cannot be accepted;
- a code of conduct in a situation where it is ensured that, in the event of the digital identification of an individual, international payments cannot be made in excess of and transaction-related and service-related sums do not exceed the limit of 2000 euros per calendar month; and
- a code of conduct for terminating a business relationship established without direct contact.

5.9. Upon the establishment of a business relationship without direct contract, the following can be used upon verifying data submitted to identify a person:

- a notarised or certified copy of an identity document submitted in writing or electronically;
- electronic methods of identification, thereby verifying the validity of the electronic signature and certificate;[37] and
- data collected by the obligated person and/or public databases for the purpose of verifying the personal identification code, registry code and data of the representatives of the company and the address.

The obligated person may use other legible documents to identify a person, including certification by other credit institutions, notaries, foreign missions, public authorities and foreign business partners.

5.10. For entry into a long-term contract with the obligated person, an appropriate attitude of the parties is presumed,[38] as a result of which obligated persons must set out constraints in their rules of procedure with the aim of avoiding unnecessary risks and ensuring the establishment of respective relationships at a suitable time and in a suitable place. In the event of business relationships established without direct contact, not only risks relating to a single transaction, but to all similar transactions and the service as a whole and their impact at the institutional level must be taken into account.[39]

5.11. The purpose of application of customer due diligence measures is not merely the identification of the customer. Sufficient application of customer due diligence measures means a situation where, among other things, the customer's risk level is determined. (Determining the customer's risk level is described in sections 4.6.5 to 4.6.8.)

---

[37] i.e. verification of the certificate of the ID card. An ID card comes with two certificates for the user: one to identify the person in an electronic environment and the other for electronic signing. The certificate can be compared to a signature specimen – it is public, and based thereon anyone can make certain that the signature is genuine. The certificate also contains personal data, including name and personal identification code.

[38] Upon entry into long-term contracts, it must be taken into account whether it is the first relationship for the person (e.g. a company, non-profit association, etc. that is about to launch operations), whether the need to enter into the long-term contract arises from another transaction (loan agreement), whether the person is a resident or non-resident etc. The adequate attitude of the obligated person calls for circumstances-based conduct for the purpose of ensuring the appropriate application of the customer due diligence measures.

[39] At the institutional level, risks arise, above all, in the event of a multitude of transactions of a certain type, whereby the credit institution and the financial institution are not able to assess the money laundering and terrorist financing risks relating to the transactions.

5.12. In the event of extraordinary termination of a business relationship on grounds resulting from § 27 of the AML/CFT Act, different time limits for provision of services (above all, restrictions on making transactions) and termination of a business relationship (long-term contract) may be established. In the event of extraordinary termination of a business relationship, the internal procedures of the obligated person must set out a procedure for the subsequent use of the customer's assets (e.g. allowing for a payment to be made to the account of a credit institution in another contracting state of the European Economic Area or in an equivalent third country). No disbursements in cash are allowed.

6. Compliance

6.1. Customer Due diligence measures

6.1.1. The requirements provided for in these Guidelines must be applied upon the establishment of and during a business relationship.[40] Customer due diligence measures must also be applied in the event of suspicion of money laundering or terrorist financing or if the obligated person has doubts about the correctness of the documents or other data submitted by a customer, i.e. when circumstances differing from ordinary behaviour and referring to the existence of risk factors of impact become evident in a customer's actions. Customer due diligence measures must also be applied in a situation where it is reasonable[41] to presume that it may constitute money laundering or terrorist financing or where the obligated person is not convinced of the sufficiency of the applied measures. The list[42] of customer due diligence measures set out in the AML/CFT Act contains the minimum criteria and is imperative. The obligated person may also take other customer due diligence measures that have not been provided by law, given the customer's field or region of activity as well as the characteristics of the transaction and related risks.

6.1.2. Obligated persons must, in addition to the customer due diligence measures provided by law, comprehensively evaluate the substance and purpose of the customer's transactions and actions, relying on the universally recognised professional skills characteristic of credit institutions and financial institutions to identify a possible link between a transaction, step or funds and money laundering or terrorist financing.

6.1.3. The obligated person has sufficiently applied the customer due diligence measures for the purposes of subsection 1 of § 13 of the AML/CFT Act if it is convinced that it has sufficiently applied the obligation arising from the aforementioned provision.[43] The principle of reasonableness is taken into account upon assessing conviction.

6.2. Customer identification

6.2.1. The *Know-Your-Customer* (KYP) principle must be followed upon customer identification. This principle means that the operating profile, purpose of operation, beneficial owner of the person

[40] For further information on the application of customer due diligence measures see subsections 1 and 2 of § 12 of the AML/CFT Act.
[41] For further information on the principle of reasonableness see § 7 of the Law of Obligations Act.
[42] The customer due diligence measures are set out in § 13 of the AML/CFT Act.
[43] For instance, in a situation where the customer's risk level is high, a generally formulated reason upon identifying the source and origin of funds cannot be considered sufficient (funds are the customer's savings, own funds, loans obtained, funds earned etc.). In the event of a high risk level, the obligated person must take enhanced due diligence measures, i.e. take additional measures to make certain that the data is correct for the purposes of subsection 3 of § 19 of the AML/CFT Act. This way the obligated person must be convinced of the legal origin of the funds based on the submitted data.

as a potential customer[44] and, if necessary, the source and origin of the funds used in the transactions and other similar information essential for the establishment of a business relationship must be identified in addition to the person. Upon making transactions, the customer must be identified and the compliance of transactions must be assessed based on the customer's main fields of activity and prior payment behaviour.

6.2.2. In line with the risk-based approach specified in section 4.6 of the Guidelines, the obligated person must choose, among other things, the suitable scope of the KYC principle.

6.2.3. Obligated persons must identify the customer and the beneficial owner within a reasonable period of time prior to the commencement of the steps for entry into a long-term contract or while entering into the contract. A person participating in the transaction must be identified prior to the commencement of the steps for entry into the long-term contract or while entering into the contract.

6.2.4. Any information and documents concerning establishment of identity must be preserved in a manner making it possible to respond fully and without unreasonable delay to relevant enquiries from the FIU, investigating body, court or supervision authority. To this end, the obligated person must set up a system enabling, in view of the characteristics of its activities, the prompt retrieval from databases and documents of the required information or document concerning identification of the customer or person participating in the transaction.

6.2.5. Identification and verification of persons upon the establishment of a business relationship are mandatory in the event of the use of any and all financial services, regardless of whether a long-term contract is entered into with the person participating in the transaction or not, thereby taking into account the exceptions arising from the AML/CFT Act.

7. Identification of individual upon establishment of business relationship

7.1. General requirements

7.1.1. The establishment and verification of the identity of an individual (a natural person) must be carried out, as a general rule, in one step on the basis of an identity document. The address, operating profile, profession and field of activity, purpose and characteristics of establishment of a business relationship, beneficial owner (if necessary) and other similar information essential for the establishment of a business relationship must be identified in addition to identifying the person.

7.1.2. An individual must be identified based on an identity document in accordance with § 23 of the AML/CFT Act. A document submitted to the obligated person for identification must be assessed as follows:

- validity of the document based on the date of expiry;
- the outward likeness and age of the person match the appearance of the person represented on the document;
- the personal identification code matches the gender and age of the submitter; and
- with respect to information contained in codes assigned to individuals of a foreign country, foreign missions or other competent authorities must be consulted in the case of doubt as to the authenticity of the document or identity.

[44] A beneficial owner is a natural person who, taking advantage of their influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed. For further information on identifying the beneficial owner see sections 7.3 and 8.3 of the Guidelines.

7.1.3. A copy of the page containing personal data and a photo must be made of the identity document in accordance with subsection 2 of § 23 of the AML/CFT Act.[45] The copy made of the document must be of a quality allowing the details included on it to be read legibly. Any details specified by law must be recorded.

7.1.4. The obligated person must register the address and profession or field of activity of the individual in the course of identification and verification of identity in accordance with subsection 3 of § 23 of the AML/CFT Acton the basis of the person's statements. As for the place of residence, not the address recorded in the population register or another similar register but the permanent or primary place of residence of the person is important. If it is difficult to determine a person's permanent place of residence (e.g. the person's place of residence cannot be identified or there are several of them), the person's habitual residence must be identified.[46] A post office box number or *poste restante* address cannot be considered a habitual residence.

7.1.5. Upon identifying the permanent place of residence or habitual residence of an individual, it is also necessary to register the address of the place to which the obligated person can send notices on paper.

7.1.6. In addition to the address of the place of residence of the individual, the obligated person may record other contact details, including an e-mail address, phone number, Facebook account, Skype account and other similar data, and agree on the submission of information via these telecommunications channels.

7.1.7. Determining field of activity, job or profession gives the obligated person the opportunity to assess whether the business relationship or transactions are in compliance with the customer's normal participation in commerce and whether the business relationship or transaction has a clear economic reason. For the purpose of prevention of the movement of illegally acquired funds, the customer's operating profile needs to be identified upon establishment of a business relationship. To this end, the customer's main fields of work and activity and possible payment habits need to be identified. It is important to pay attention to persons with whom the customer enters into transactions and to their seat.

7.1.8. Upon identifying an individual, it must be identified whether the person is a politically exposed person[47] .

7.1.9. Any details and references required to identify a person must be verified by means of reliable and independent sources of information (e.g. national registers, authorities, credit institutions, foreign missions of the Republic of Estonia and foreign missions in the Republic of Estonia or based on documents and other information certified by other relevant authorities). In exceptional instances[48] (if the use of reliable and independent sources of information is impossible), copies of documents or information communicated by unofficial representatives or mediators or other dependable information (incl. handwritten statements by a person) may be relied on to identify a person. The obligated person must, prior to entering into transactions or taking steps with the person to be identified, make certain that the information obtained in such a manner is sufficient. In such an instance, a notation to this effect must be made on the copies confirming identification, and thereafter the legality of the details and documents must be verified immediately.

[45] Instead of making a copy, the data displayed using the ID card administration application (incl. a photo) can be recorded.

[46] A person's habitual residence is the place where the person wants to be and to which the person is connected. The habitual residence of a person is not simply the place where the person permanently or mainly resides. The person's intentions and future plans relating to staying in a specific country or place are also important upon identifying habitual residence. It is an autonomous term and does not depend on national substantive law.

[47] For further information on politically exposed persons see section 7.2 of the Guidelines.

[48] Such instances must be regulated by the internal procedure rules of the obligated person. Relevant documents must provide information about the exception.

7.1.10. The identification or recommendation of a person by the executives, other customers or business partners of the obligated person may contribute to the identification of the customer, but the respective recommendations do not substitute for the identification requirements contained in the AML/CFT Actor release the obligated person from the fulfilment of the requirements.

7.1.11. Even if the obligated person knows the customer personally or the customer is a public figure, the internal identification procedure provided by law cannot be disregarded. The identity of the public figures and persons directly or indirectly related to them who address the obligated person for performance of transactions or taking of steps must be verified.

7.1.12. In the event of persons whose active legal capacity is limited (incl. minors), the obligated person must also follow the identification procedure. Upon identification of the personal data of minors, the obligated person must, in addition to the instructions given in these Guidelines and provisions of the AML/CFT Act, follow the provisions of the General Part of the Civil Code Act and the Family Act. In addition to the personal data of a person of restricted active legal capacity, the personal data of the legal representative (parent(s) or guardian(s)) must be verified.

7.1.13. In the case of the representation of an individual, the requirements provided for in section 8.2 must be followed and applied to the individual to the appropriate extent.

7.1.14. The identification of a customer is not a one-off step. The obligated person must regularly update the customer's personal data and operating profile, ensuring that they are up to date and based on the customer's risk level.[49]

7.2. Politically exposed persons

7.2.1. The obligated person must establish internal procedures in order to decide whether a potential customer or its beneficial owner is a politically exposed person[50] of a contracting state of the European Economic Area or third country, a domestic politically exposed person or a person who is or has been entrusted with a prominent function by an international organisations.

7.2.1.1. Obligated persons must identify the close associates and family members of politically exposed persons only if their link to a person carrying out significant duties of public authority is known to the public or if the obligated person has reason to believe that such a link exists.

7.2.1.2. With regard to politically exposed persons, obligated persons must take the following measures in addition to relevant customer due diligence measures:

- request the required information from the customer, incl. take immediate measures to identify the sources of wealth and funds used in the framework of the business relationship or transaction;
- collect data or make an enquiry with the respective databases[51] or public databases[52]; or
- make an enquiry or verify information on the webpages of the relevant supervision authorities or institutions in the country of location of the customer or person.

[49] In the case of higher-risk customers it is advisable to update any documents serving as the basis for identification at least once a year.
[50] Under subsection 1 of § 20 of the AML/CFT Act, a politically exposed person is an individual who performs or has performed prominent public functions, as well as their family members and close associates.
[51] Various databases (e.g. WorldCheck) include information for the identification of politically exposed persons.
[52] Public databases also include information available online about politicians and cabinet members.

7.2.2. The establishment of a business relationship with a politically exposed person must be decided by the management board of the politically exposed person or the person(s) authorised by the management board. If a business relationship with a customer has been established and the customer or the beneficial owner later proves to be or becomes a politically exposed person for the purposes of section 7.2.1 of the Guidelines, the management board (or persons authorised by the management board) must be informed.

7.2.3. The obligated person must exercise regular enhanced supervision in business relationships established with a politically exposed person (except in cases provided by law).

7.2.4. Regular supervision must also be exercised by the obligated person after a politically exposed person has ceased to be a politically exposed person if the obligated person feels, based on the risk-based approach, that the person still entails a higher risk.

7.3. Identification of beneficial owner of individual

7.3.1. Upon identifying an individual, the obligated person must, in the event of doubt, also identify the beneficial owner of the individual, i.e. the person who controls the actions of the individual.

7.3.2. A doubt about the existence of a beneficial owner may arise, above all, if the obligated person perceives, upon applying customer due diligence measures[53] , that the individual has been swayed[54] to establish the business relationship or enter into the transaction. In such an event the person who exercises control over the individual must be deemed the individual's beneficial owner.

7.3.3. It must be taken into account that the scope of customer due diligence, including upon identifying the beneficial owner, is related to the risk of money laundering and terrorist financing, which depends on the type of customer, its country of origin, business relationship, product, service or transaction.

7.4. Civil law partnerships and other contractual associations

7.4.1. Upon identification of civil law partnerships,[55] all of the members of the partnership or their representatives must be identified on the grounds applicable to individuals. The beneficial owners of the partnership must be identified.

7.4.2. In the case of civil law partnerships, the purpose of their activity and, if necessary, the origin of the funds used must be identified. Thereby one may rely, among other things, on clarifications and statements given by the representative of the partnership. The obligated person must make sure that the use of funds by the partnership corresponds to the purposes of activity declared by it previously.

7.4.3. Data of the members of the partnership and their representatives must be preserved and regularly updated.

---

[53] For instance, it becomes evident in the identification process that the data is not correct, the source and origin of funds is doubtful, information gathered upon the establishment of the business relationship proves to be wrong when making occasional transactions etc.

[54] 'Inclined' means beguiled, asked, threatened, bribed, taken advantage of, incl. controlled the used person by way of dominant knowledge, will or organisational power apparatus, or the intent of the person has been otherwise kindled.

[55] For further information on the legal nature of civil law partnerships see § 580 *et seq* of the Law of Obligations Act.

8. Identification of legal entity upon establishment of business relationship

8.1. General requirements

8.1.1. The business name, registry code, seat and place of business, information about the legal form, passive legal capacity, representatives (legal representatives and those authorised to represent the legal entity before the obligated person)[56] and beneficial owners must be identified upon identifying legal entities. The operating profile, business partners, purpose of operation, purpose of establishment and characteristics of business relationships and other similar information required for the establishment of business relationships must be identified as well.

8.1.2. Upon determining the seat of a legal entity, both the theory of the country of foundation[57] as well as the theory of the seat[58] must be used to identify whether the legal entity may involve country and geographical risks for the purposes of section 4.6.4.3.

8.1.3. The place of business of a legal entity must be determined on the basis of factual circumstances, i.e. where production is based or a service is provided.[59]

8.1.4. The identification and verification of the identity and passive legal capacity of a legal entity must be carried out, as a general rule, on the basis of the information contained in the commercial register (in Estonia) or another equivalent register or a copy of the registration certificate or an equivalent document (for instance, in countries where there is no national register, foundation documents certified by a notary are considered equivalent) submitted in accordance with the procedure provided by law. Documents issued by a register or their equivalents must have been issued no earlier than 6 months prior to their submission to the obligated person.

8.1.5. Documents issued in a foreign state must be legalised or apostilled,[60] i.e. in order to use an official document issued in one country in another, an internationally recognised certificate of the authenticity of the document[61] is given in another.

8.1.5.1. Documents issued by Lithuanian, Latvian, Polish, Ukrainian or Russian authorities and officials do not require legalisation[62] or an apostille.

8.1.5.2. To be legalised, a document must go through the legalisation authorities[63] of the issuing state as well as those of the receiving state (usually, foreign ministries).

---

[56] All individuals acting on behalf and on account of a legal entity who are entitled to dispose of the funds of the entity must be identified in accordance with the requirements provided for in § 23 of the AML/CFT Act and these Guidelines.

[57] According to the theory of the country of foundation, the country where a legal entity was founded is the country of location of the legal entity.

[58] According to the theory of the seat, the seat of a legal entity is the country where the entity is actually located (i.e. the seat of the management board or the body substituting for it).

[59] If a service is only provided online, the place of provision of the service (place of business) is the country where the service is available.

[60] Apostilles are made in accordance with the Hague Convention of 5 October 1961, *Abolishing the Requirement of Legalisation for Foreign Public Documents* (hereinafter the Convention), by which the contracting states have waived more complex legalisation and replaced the procedure with apostilles, which are simpler. The list of contracting states is available at www.hcch.net. Documents reaching Estonia from these countries must have been certified with an apostille (a certificate of issue by a competent officer) by a respective foreign authority.

[61] The person making the apostille is not liable for the correctness of the information contained in the document, but certifies the authenticity, i.e. the authenticity of the signatures (see Article 2 of the Convention: "…*legalisation means only the formality by which the diplomatic or consular agents of the country in which the document has to be produced certify the authenticity of the signature, the capacity in which the person signing the document has acted and, where appropriate, the identity of the seal or stamp which it bears").*

[62] Documents originating from countries that have not joined the Convention (e.g. Canada) need to be legalised.

8.1.6. Upon identification, legal entities are not required to submit an extract of their registry card if the obligated person has access to the required extent via the computer network to the data in the commercial register or register of non-profit organisations and foundations (including access to data in respective registers in the foreign country).

8.1.7. Upon identification of a legal entity, the obligated person is required to register the names[64] of the executive of the legal person or members of its management board or another body substituting for it, their powers in representing the legal entity and the principal field of activity of the legal entity. If the aforesaid details are not indicated by the register extract or another relevant document, the relevant information must be obtained by using other documents and/or reliable sources of information.

8.1.8. The need for use, the criteria of use and/or the list of reliable sources of information must be specified by the obligated person (e.g. information issued by national registers, public authorities, credit institutions, foreign missions of the Republic of Estonia and foreign missions in Estonia may be used).

8.1.9. The obligated person must identify the existence of politically exposed persons related to the legal entity.[65] If no respective links appear in the information about a politically exposed person obtained from the representative of the legal entity, an enquiry must be made with the respective databases in the event of suspicion.

8.1.10. In the case of international organisations, the documents serving as the basis for their activities (including in Estonia) must be determined and the submission of relevant documents must be requested. If necessary, information required for the establishment of the business relationship which is contained in the documents must be verified.

8.2. Agency

8.2.1. The obligated person must verify if the person is acting on their own behalf or on behalf of another (natural or legal) person. If the person is acting on behalf of another person, the obligated person must also identify the person on behalf of whom transactions are performed.

8.2.2. Documents required to identify a legal entity must be submitted by the legal representative or authorised representative of the entity. The obligated person must make certain that the right of representation complies with legislation.[66] If the submitted documents do not indicate the right of representation of the individual submitting them and/or the authority is not compliant, the identification process (and thus also the establishment of the business relationship or performance of the transaction) cannot be continued.

---

[63] For further information on legalisation, see the website of the Estonian Ministry of Foreign Affairs (http://www.vm.ee/?q=taxonomy/term/39). Among other things, the Estonian Foreign Ministry legalises documents issued in Estonia.

[64] In accordance with § 65 of the Commercial Code, management board members and their rights in representing the company are recorded on the B card; however, documents issued by the relevant registers in foreign countries and equivalent documents do not always indicate the details of the members of the management board of the legal entity or the body substituting for it.

[65] For further information on identifying politically exposed persons see section 7.2 of the Guidelines.

[66] Usually, it is presumed that the legal person is represented by a legal representative or an authorised person. In the case of powers of attorney and other documents made abroad, it must be taken into account that these need to be either legalised or issued with an apostille (see section 8.1.5 herein).

8.2.3. The obligated person must identify the basis, scope and term of the representative's right of representation. The representative must be asked to submit a document proving the right of representation. Further attention[67] must be paid to the verification of the identity and right of representation of authorised representatives operating or residing in a jurisdiction different from the legal entity's jurisdiction or whose rights of representation are valid for more than a year.

8.2.4. Clarification must be sought on the scope of the right of representation granted to the authorised representative (for instance, whether a one-off transaction or recurring transactions over a certain period are involved). The obligated person must take notice of the terms of the right of representation granted to the authorised representative and provide services only to the extent of the right of representation.

8.2.5. Under subsection 5 of § 23 of the AML/CFT Act, the obligated person has the right to request that the representative of a legal entity of a foreign country submit documents proving their right of representation, notarised or certified in an equivalent manner and legalised or certified with an apostille, unless provided for otherwise in an international agreement.

8.2.6. Upon handling the right of representation of authorised and legal representatives, it must be made certain whether the representative knows their customer.[68] To identify the true nature of the relationships between the representative and the represented, the representative must know the substance and purpose of the declarations of intent by the represented party and be able to answer other relevant questions about the seat of operations, fields of activity, sales and transaction partners, other related persons and beneficial owners. In addition, the representative must confirm with their signature that they are aware and convinced of the source and legal origin of the funds used in the transaction of the represented.

8.3. Identification of beneficial owner

8.3.1. Upon the identification of a legal entity, the obligated person must register the beneficial owner of the entity.[69]

8.3.2. In a situation where no person holds or identifiably controls more than 25%, the circle of beneficial owners will be identified pursuant to the principle of proportionality, according to which information must be requested about the shareholders, partners and other persons who exercise control or other significant influence over the activities of the legal entity.

8.3.3. If the identification documents of a legal entity or other submitted documents do not indicate the beneficial owner of the entity, the relevant information (including information about membership of the group of companies and the ownership and management structure of the group of companies) must be registered on the basis of the statements or a handwritten document of the representative of the entity.

8.3.4. In order to verify information identified on the basis of statements or a handwritten document,[70] reasonable measures must be applied (e.g. the filing of a query with relevant registers) and the

[67] Upon handling a document containing representation rights, it must be identified whether the issuers had the required competence.

[68] A person representing a legal entity is expected to be familiar with the person's economic and professional activities, purposes of transactions, partners, source and origin of funds used in transactions, circle of owners etc.

[69] The term 'beneficial owner' also includes the shareholders in a company that are individuals who hold or exercise control over more than 25% of the shares or voting rights by means of direct or indirect ownership (a person who holds more than 25% of the shares in the company and is considered the beneficial owner), including in the form of bearer shares, also shareholders in a company who are natural persons who exercise control over the management of the company in another manner. Voting rights can be identified and the term 'control' can be substantiated based on § 10 of the Securities Market Act. If it is a company whose securities have been listed on a regulated securities market, the identification of the beneficial owner of such a company will not be necessary.

submission of the annual report or another relevant document of the legal entity must be requested.

8.3.5. The obligated person may use a risk-based approach and take sufficient measures to verify the identity of the beneficial owner with the aim of making certain as to whom the beneficial owner in the business relationship or transaction is. With respect to compliance with this requirement, obligated persons are left with several options in order to decide:

- the extent to which public information about shareholders or members will be used;
- the extent to which relevant information will be requested orally or to record obtained information in writing or in a form that can be reproduced in writing;
- in which cases the customer will be asked to complete a respective questionnaire; or
- what other options can be used and are practicable in the event of the respective obligated person.

8.3.6. It must be taken into account that the scope of customer due diligence with respect to the customer (incl. identification of the beneficial owner) is related to the risk of money laundering and terrorist financing, which depends on the type of customer, their country of origin, business relationship, product, service and transaction.

8.3.7. Higher attention must be paid to companies founded in territories with a low tax rate, whose beneficial owners are often difficult to identify.

8.3.8. The obligated person can consider a person who exercises control in another manner, without having a 25% shareholding in the company, as the beneficial owner. This situation arises when the obligated person suspects that a third party whose links to a company cannot be legally proven or are difficult to prove the exercises of control over management of a legal person.

8.4. Requirements for identification of non-resident legal entities

8.4.1. In the event of the identification of legal entities that are non-residents, the obligated person must comply, to the greatest extent possible, with the same requirements as in the event of customers that are residents, taking into account the specifications arising from the country of origin and legal form of the non-resident customer. Due to differences in legal regulations in different countries, the rules of procedure of the obligated person must also set out detailed requirements and guidelines for the identification of the passive legal capacity of the legal entity by means of other documents and/or reliable information sources.

8.4.2. Upon identifying the passive legal capacity of a non-resident legal entity and handling documents certifying the powers of representatives, it must be verified whether the documents meet the requirements established in Estonian legislation with respect to legalisation of foreign documents.[71]

8.4.3. Due to differences in legal regulation in different countries, the obligated person must pay attention, above all, to companies founded in countries or territories with a low tax rate,[72] because it is not always abundantly clear whether they have passive legal capacity. In many countries, the standards for identifying a customer and registration and preservation of documents are lower than in Estonia, as a result of which particular attention must be paid to the

---

[70] Upon acceptance of a customer's statements or handwritten document, the customer must be informed of the liability arising from giving misleading or false information.
[71] See footnotes 60-63.
[72] List of tax-free and low-tax territories (footnote 19).

content of the documents of the companies registered in such countries and to the manner of their submission.[73]

8.4.4. Particular attention must be paid to information and documents submitted in the case of persons whose country of origin is on the FATF's list of countries that do not contribute sufficiently to the prevention of money laundering.[74]

8.4.5. In the event of foreign-language documents, the obligated person is entitled to request a translation of the documents into a language understood by it. The use of translations should be avoided in a situation where the original documents have been prepared in a language understood by the obligated person (e.g. the translation of English-language original documents into Russian).

9. Application of customer due diligence measures upon execution of transactions

9.1. General requirements

9.1.1. In addition to the establishment of a business relationship, customer due diligence measures must also be taken if:

9.1.1.1. in the event of any kind of transaction, incl. in the event of an offer made in the course of provision of a counselling service whose price exceeds the limit specified in the AML/CFT Act.[75] Thereby it is irrelevant whether the pecuniary obligation is performed by means of cash or cashless settlements;

9.1.1.2. the amount of a single transaction or the total amount of consecutive transactions exceeds the limit provided by law (or the internal procedure rules of the obligated person).[76] The obligation must be performed upon occasional[77] transactions made by a non-customer;

9.1.1.3. the obligated person has doubts about the correctness or sufficiency of the data collected upon establishment of the business relationship and if the actions of the other party are not ordinary or transparent as well as if the obligated person suspects money laundering or terrorist financing; and

9.1.1.4. the obligated person does not suspect money laundering or terrorist financing for the purposes of subsection 1 of § 32 of the AML/CFT Act and does not have the reporting obligation for the purposes of subsection 3 of § 32 of the AML/CFT Act, but the transaction is complex and extraordinarily large or the transaction scheme is unusual and does not have an obvious economic or legal purpose.

9.1.2. The obligated person must constantly assess changes in the customer's operations and whether these may raise the risk level so that additional customer due diligence measures need to be taken.

9.1.3. The application of customer due diligence measures also calls for the existence of the respective monitoring systems whose purpose is to detect reaching the transaction limit or the existence of

[73] See section 8.1.5 of the Guidelines.
[74] The list of uncooperative countries with high risk of money laundering (footnote 26).
[75] If the limit specified by law or rules of procedure is reached by way of several consecutive transactions rather than the first transaction, customer due diligence measures must be applied immediately once reaching the limit becomes evident.
[76] See subsections 4^3, 5, 6, 7 and 8 of § 15 of the AML/CFT Act.
[77] Occasional transactions are transactions whereby no business relationship for the purposes of law is established, but the same persons participate in the transaction, repeatedly taking similar action (e.g. currency exchange; one-off (international) payments; transactions with travel; and tax-free, bonus and other cheques of foreign institutions).

risk factors and inform the appropriate persons thereof for the purpose of identifying suspicious or unusual transactions. If the obligated person comes to suspect money laundering in the course of monitoring transactions, the FIU must be informed thereof.

9.2. Following transactions

9.2.1. The following of unusual and suspicious transactions is an important part of the set of customer due diligence measures applied by financial institutions and allows for the identification of circumstances that may point to money laundering or terrorist financing in the economic activities of customers. Also, the purpose of following a customer's transactions is to identify transactions with subjects of international sanctions and politically exposed persons and detect and notify of transactions whose limit or other parameters exceed the prescribed value over a certain period of time.

9.2.2. Transaction-following measures can be divided into two. One can use measures which enable, based on parameters or features developed with the help of the obligated person's prior work experience, transactions to be followed in real time[78] as well as analysed afterwards.[79]

9.2.3. Screening

9.2.3.1. In the event of following transactions in real time, customer executives or other bank employees observe, upon performing their duties, the customer's behaviour and transactions with the aim of detecting unusual or suspicious transactions or transactions exceeding the prescribed limits.

9.2.3.2. Upon following transactions in real time, information technology tools which, using predefined parameters, select transactions made over a certain period must be used. The screening parameters depend on information technology possibilities and established goals. What must be identified is as follows:

- politically exposed persons involved in transactions;
- transactions with persons whose name, date of birth etc. match data disclosed in lists of persons subject to international sanctions;
- transactions with persons whose country of operation or origin is included on the list of higher (terrorist) risk countries; and
- persons whose transactions are subject to one-off temporary monitoring.

9.2.4. Monitoring

9.2.4.1. Upon monitoring transactions, measures must be taken to verify the submission of information required about the payer upon money transfer. In order to help detect suspicious transactions, payment service providers should take measures to detect the absence of payer-related information in payment instructions.

9.2.4.2. With the help of monitoring systems, the recipient's payment service provider must check whether the reporting or payment and settlement system fields used for making the transaction have been filled with the symbols or input used in the reporting or payment and settlement system with regard to the information relating to the payer.

9.2.4.3. Using monitoring systems, payments with insufficient data about the payer (incl. the payer's name, address and account number) must be identified among the payments of the payment service provider of the payer. Thereby the payer's address can be replaced with the payer's date and place of birth, customer number or personal identification code,

[78] Screening.
[79] Monitoring.

and if the payer does not have an account number, the payment service provider of the payer will replace it with a unique feature with the help of which the payer can be identified.

9.2.4.4. For the purpose of analysing transactions afterwards (monitoring), one can analyse transactions separated from the mass of transactions based on predefined parameters. Transactions it is not possible to interfere with during execution (e.g. transactions made via an ATM) are the main objects of monitoring. In addition, upon subsequent monitoring of transactions, the largest transactions based on the sum, currency and customer type over a certain period are analysed. A list of typical parameters[80] on the basis of which transactions can be selected for monitoring is given below:

- single large international payments (e.g. whereby the sum ends with at least four zeros);
- international payments whose description contains the words 'loan', 'deposit', 'payback' etc.;
- accounts (of individuals and legal entities) with the highest turnover in the period under review based on currencies (of individuals and legal entities);
- the largest transactions (of individuals and legal entities) in the period under review (of individuals and legal entities) based on different currencies;
- transactions made via an ATM which exceed a certain limit over the period under review;
- cash withdrawals in a bank branch based on currencies as well as individuals and legal entities which exceed a certain limit;
- single transactions that exceed the limit, which are made by customers whose turnover is small;
- sudden upsurge in turnover of holders of correspondent banks' VOSTRO accounts;
- transactions with persons whose country of operation or origin is on the list of higher (terrorist) risk countries;
- payments to high-risk countries;
- payments relating to risky banks; and
- transactions of specific customers or customer types.

9.2.5. If the payment service provider of the recipient notes that the required information about the payer is missing or incomplete upon receiving a payment, the recipient must refuse the transaction or request full information about the payer.

9.2.6. If the customer is regularly unable to give the requested information about the payer, the obligated person must take measures which include giving warnings and setting time limits. Thereafter the recipient may refuse to enter into any transactions with the customer or limit or terminate the business relationships with the customer. The payment service provider of the recipient informs the FIU thereof.

10. Conduct in case of suspicion of money laundering and fulfilment of reporting obligation

10.1. In a situation where the obligated person, based on documents collected in the course of application of customer due diligence measures, develops a suspicion of money laundering or terrorist financing upon the establishment of a business relationship or upon occasional making of transactions, the obligated person is not permitted to establish the business relationship or make the occasional transaction.

[80] The obligated person may use other transaction-following principles.

10.2. If unusual circumstances or circumstances whereby an employee of the obligated person suspects money laundering or terrorist financing[81] become evident in relationships with a customer,[82] the compliance officer appointed by the executive/management board must be immediately informed thereof and the compliance officer will decide the immediate forwarding of the information to the FIU[83] and the need to postpone or refuse to make the transaction. In a situation that entails a high risk of money laundering or terrorist financing, an employee of the obligated person may decide to postpone the transaction and thereafter inform the compliance officer of the situation.

10.2.1. The background of each individual suspect or unusual instance must be investigated as much as reasonably necessary, thereby recording the details of the transaction and analysing the circumstances with the aim of identifying the typical features of more frequent transactions.

10.2.2. The main circumstances to which attention should be paid when suspect and unusual transactions are analysed are as follows:

- What is suspicious about the steps, transactions or other circumstances?
- Is the obligated person convinced that it knows its customer sufficiently or is it necessary to collect additional information about the customer?
- Upon taking a step or making a transaction involving identifying a customer or the customer's representative, the obligated person must make certain that it follows the prescribed procedure. Was all the required information submitted or did additional information need to be requested or otherwise clarified?
- Have there been repeated instances of suspicious steps and transactions?

10.3. If the postponement of a transaction could cause significant losses to the parties, its omission is impossible or may prevent the interception of the potential perpetrator of money laundering or terrorist financing, the transaction or official act must be performed and thereafter a report must be forwarded to the FIU.

10.4. The rules of procedure of the obligated person must set out a code of conduct for the staff of the obligated person regarding the postponement of a transaction or official act.

10.5. The rules of procedure of the obligated person must set out both the conditions for the forwarding of information to the FIU as well as for the preservation of the forwarded information.

10.6. The obligated person must preserve in a form that can be reproduced in writing all of the information received from staff about suspicious or unusual transactions and any information collected to analyse these reports and other related documents and any reports forwarded to the FIU along with information about the time of the forwarding of the report and the employee that forwarded it.

10.7. No customer or party participating in a transaction (including its representative or other related parties) with respect to whom suspicion is being communicated to the FIU may be notified of this.

10.8. The obligated person must immediately fulfil the reporting obligation. The purpose of immediate fulfilment is to give the FIU the chance to develop the suspicion specified in subsection 1 of § 40 of the AML/CFT Act and for taking its own measures. Money laundering is a process where

[81] In addition to the FIU guidelines described in footnote 82, the obligated person will, based on its prior work experience, make a list of the extraordinary and unusual behaviour of the customer and describe the elements of circumstances that spark suspicion of money laundering and terrorist financing.

[82] See the advisory guidelines of the FIU regarding transactions involving suspicion of money laundering. Available at http://www.politsei.ee/dotAsset/258252.pdf (05.06.2013).

[83] In accordance with clause 2 of subsection 3 of § 31 of the AML/CFT Act, one of the duties of the contact person is the communication of information to the FIU in the event of suspected money laundering or terrorist financing. The FIU is in the area of administration of the Ministry of the Interior and is a stand-alone structural unit of the Central Criminal Police. For further information see the FIU's website at http://www.politsei.ee/et/organisatsioon/rahapesu/ (05.06.2013).

criminal proceeds, above all, financial assets may be transferred via credit institutions and financial institutions of multiple states in a single day and therefore swift reporting helps to track down illegal funds more effectively.[84]

11. Correspondent relationships

11.1. In order to establish a correspondent relationship with a credit institution or financial institution of a third country, the obligated person must obtain consent from the management board and, for the purpose of application of enhanced due diligence measures:

- collect sufficient information about the correspondent institutions in order to fully understand the nature and reputation of the business operations of the institution; also obtain certification as to the quality of exercising supervision over it. Any possible connection of the correspondent institution with a suspicion of money laundering or terrorist financing, relevant investigation steps or sanctions must be checked in public sources;
- evaluate the institution's mechanisms for the prevention of money laundering and terrorist financing and make certain that these are adequate and effective; and
- document the obligation/responsibility of both parties to the correspondent relationship in the field of the prevention of money laundering and terrorist financing, including the exchange of relevant information (entry into a relevant contract[85]).

11.2. The contract for a correspondent relationship entered into with a credit and financial institution from a third country or the rules of procedure of the relevant obligated person must set out the obligations of the parties, including the conditions for the application of customer due diligence measures to payable-through accounts, i.e. correspondent accounts to which a third party has direct access to effect transactions in its name,[86] with respect to customers with access.[87]

11.3. The obligated person is not allowed to open a correspondent account in a so-called shell bank or a bank where a shell bank has accounts. Correspondent accounts must not be opened in a bank where evaluation of the reliability of executives and of measures to prevent money laundering and terrorist financing uncovers deficiencies in view of relevant international standards or the circumstances serving as the basis for evaluation.

11.4. The obligated person is forbidden to establish a correspondent relationship with an institution or company in any other third country that is not a credit institution or financial institution under Estonian law, yet whose principal and sustained business activity is similar to banking[88].

---

[84] For instance, in a situation where the obligated person performs a transaction whereby it disburses cash to the customer or the person participating in the transaction, the disbursed cash becomes invisible, because further movement of the funds is virtually impossible to track. Therefore, in a normal situation and, above all, in a situation where cash is disbursed to the customer or a person involved in the transaction which may involve the impossibility of following the funds further, the obligated person has the obligation to report thereof immediately, i.e. before the transaction is made, if possible.

[85] If a relevant provision is not included in the terms and conditions of the institution (correspondent bank) providing the service, the relevant obligations will be regulated in a separate agreement.

[86] Payable-through accounts.

[87] Such an obligation results from the circumstance that many credit institutions offering payable-through accounts are in reality unable to identify or forward to competent law enforcement authorities any information on the parties using such accounts.

[88] An institution or undertaking that provides customers with the execution of transactions similar to the transactions referred to in subsection 1 of § 6 of the Credit Institutions Act but which is not subject to state supervision

12. Foreign affiliates and subsidiaries

12.1. Obligated persons registered in Estonia apply customer due diligence measures and the requirements for information collection and preservation that are at least equivalent to the provisions of the AML/CFT Actin all foreign offices, branches and majority-held subsidiaries of the companies of the consolidation group.

12.2. If the legislation of the third country does not permit the application of equivalent measures, the credit and financial institutions must notify the Financial Supervision Authority of this immediately and apply supplementary measures to prevent money laundering or terrorist financing.

12.3. Obligated ersons operating in several different countries, including in a third country, must avoid in their activity the application of standards differing by country. Standards approved in the European Union provide guidance.

Annex 1

to 'Measures for the Prevention of Money Laundering and Terrorist Financing in Credit Institutions and Financial Institutions' – Advisory Guidelines of the Financial Supervision Authority (hereinafter the Guidelines)

This Annex sets out the risk assessment model, taking into account section 4.6 of the Guidelines of the Estonian Financial Supervision Authority.

Four categories associated with the person participating in the transaction must be taken into account upon risk assessment:

I. **place of residence[89] or seat[90] of the person participating in the transaction** – country and geographical risks must be taken into account;

II. **parameters characterising the person participating in the transaction** – customer risk must be taken into account;

III. **economic activities of the person participating in the transaction** – product and service risks must be taken into account; and

IV. **transaction partners of the person participating in the transaction and risks related to them** – the customer risk of the transaction partners of the person participating in the transaction, the country and geographical risks and the product and service risks must be taken into account.

Upon assessment of these risks, each risk category must be assessed on a scale of 3 points where:

the risk is low –	There are no risk factors of impact in any risk category and the customer and the customer's operations are transparent and do not deviate from the operations of an average, reasonable person engaged in the same field. Thereby there is no suspicion that the risk factors on the whole might cause the realisation of the threat of money laundering or terrorist financing.
the risk is medium –	There is one risk factor or there are several risk factors in the risk category, which differ(s) from the operations of a person engaged in the same field, but the operations are still transparent. Thereby there is no suspicion that the risk factors could, on the whole, cause realisation of the threat of money laundering or terrorist financing.
the risk is high –	There is one feature or there are several features in the risk category which, on the whole, undermine the transparency of the person and the person's operations, as a result of which the person differs from a person operating in the same field. Thereby the realisation of the threat of money laundering or terrorist financing is at least possible.

[89] See section 7.1.4 of the Guidelines.
[90] See section 8.1.2 of the Guidelines.

Next, the score should be totalled, attributing the coefficient of 2 to category 4. Thereafter the total amount should be divided by 4. The average of the categories determines whether the risk category of the person participating in the transaction is high, medium or low.

Example: The seat of the person participating in the transaction is Estonia. It is a domestically operating company engaged in providing construction services to Estonian customers.

Risk level / Risk category	Low Score – 1	Medium Score – 2	High Score – 3	Coefficient	Impact on risk level
1. Place of residence or seat of person participating in transaction	1			1	1
2. Parameters characterising person participating in transaction	1			1	1
3. Economic activities of person participating in transaction	1			1	1
4. Transaction partners of person participating in transaction and persons related to them	1			2	2
Average					1.25

If the average of the categories is under 2, it should be noted that the customer cannot have a low risk category if at least one of the categories has a high risk. The customer's overall risk category is also high if a risk factor as such calls for this (see section 4.6.8.1 of the Guidelines).

Parameters of determining customer's risk level

- the customer's risk level is low – $x < 2$
- the customer's risk level is medium – $2 \leq x \leq 2.75$
- the customer's risk level is high – $x > 2.75$