Advisory guidelines of Finantsinspektsioon
'Application of international financial sanctions in credit and financial institutions'

Advisory guidelines have been established with Resolution No 1.1-7/177 of the Management Board of Finantsinspektsioon of 25.10.2021

CONTENTS

1. Competence of Finantsinspektsioon

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

1.2. According to subsection 30 (1^1) of the International Sanctions Act (hereinafter *ISA*), Finantsinspektsioon exercises supervision over compliance with the ISA and the legislation adopted on the basis thereof by credit institutions and financial institutions that are subject to its supervision under the FSAA and in accordance with the legislation of the European Union. Finantsinspektsioon exercises supervision in accordance with the procedure provided for in the FSAA, taking account of the variations provided for in the ISA.

1.2.1. The task of Finantsinspektsioon in applying financial sanctions is not to make exceptions or allow the provision of a service or the performance of a transaction or an act. Among other things, Finantsinspektsioon does not check whether a person is the subject of a financial sanction, whether it is a transaction or an act violating a financial sanction and whether the financial sanction has been applied lawfully.

1.2.2. The task of Finantsinspektsioon when applying financial sanctions is to supervise the compliance of the systems and controls applied by a person having specific obligations so that the person having specific obligations is able to apply the financial sanction and assess the risk of the financial sanction (threats, vulnerabilities, compensation mechanisms).

1.3. These advisory guidelines (hereinafter the *Guidelines*) must be read in conjunction with the advisory guidelines of Finantsinspektsioon 'Organisational solutions and preventive measures for credit and financial institutions to take against money laundering and terrorist financing' [1](hereinafter *AML Advisory Guidelines of Finantsinspektsioon),* taking into account the variations of international sanctions. In all matters not regulated by the Guidelines, the AML Advisory Guidelines of Finantsinspektsioon shall be applied.

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

2. Purpose, scope, and basic principles

2.1. Purpose

2.1.1. The purpose of the Guidelines is to provide explanatory instructions for the application of financial sanctions. When the Guidelines refer to obligations or a sanction in general and its application, it is precisely the activities for the application of the financial sanction that are kept in mind. Consequently, the Guidelines do not cover, *inter alia*, the application of trade sanctions as a sub-category of economic sanctions. Nevertheless, the persons having specific obligations must be aware of the operational and other risks concerning their activities and properly assess and treat them in the interests of their clients.

[1] Available online at: https://www.fi.ee/sites/default/files/2018-11/FI_AML_Soovituslik_juhend.pdf. (04/01/2021)

2.1.2. The purpose of the Guidelines is to help increase the ability of persons having specific obligations under the supervision of Finantsinspektsioon to apply financial sanctions and identify the subject of financial sanctions with the ultimate goal of ensuring application of a financial sanction established with the United Nations (hereinafter *UN*) Security Council Resolution, decision of the Council of the European Union (hereinafter *EU*), regulation of the Government of the Republic of Estonia (hereinafter *Government of the Republic*) or other legislation or agreement imposing obligations on Estonia through the compliance framework for a person having specific obligations. The Guidelines are limited to financial sanctions, the application of which is binding in Estonia.

2.1.3. The Guidelines explain to persons having specific obligations the content of and compliance with the requirements for the application of financial sanctions stipulated in the ISA and legislation directly related thereto, as well as the understanding of the risks associated with the provision of service. These also guide and assist the person having specific obligations in building and ensuring the functioning of a risk mitigation and risk management system of the sanction for the purpose of applying the financial sanction.

2.1.4. The establishment and implementation of the Guidelines by persons having specific obligations will help to more effectively identify the subject of a financial sanction, apply the measures of the financial sanction, reduce the likelihood and systemic risks of the Estonian financial sector being exploited for criminal purposes and increase the stability, reliability, and transparency of the financial sector.

2.2. Scope

2.2.1. The Guidelines are addressed to credit and financial institutions providing services in Estonia, which are persons having specific obligations pursuant to subsection 20 (1) of the ISA and in terms of compliance with the requirements provided for in section 21, and which are subject to supervision by Finantsinspektsioon (hereinafter *person having specific obligations*).

2.2.2. Finantsinspektsioon may establish annexes to the Guidelines, the purpose of which is to provide sector-specific instructions to persons having specific obligations in identifying the risks associated with the provision of their services. Finantsinspektsioon may amend or supplement the technical annexes of the Guidelines, except for the sector-specific guidelines specified in this clause, without involving market participants or other experts.

2.3. Basic principles

2.3.1. Pursuant to sections 3 and 4 of the ISA, the sanctions established by the EU, the UN, and the Government of the Republic are binding in Estonia. For the purposes of the Guidelines, the sanctions imposed by the EU, the UN, and the Government of the Republic relating to financial sanctions are important.

2.3.2. Resolutions adopted by the UN, imposing sanctions, are implemented in Estonia mainly through the EU legislation and, if necessary, the Government of the Republic may issue legislation implementing the sanctions imposed by the UN. A sanction established by the UN Security Council resolution shall be applied provisionally on the basis of the UN Security Council resolution until the regulation of the Council of the European Union is updated or adopted. In addition, the EU can supplement the UN sanction and impose an autonomous EU sanction.

2.3.3. A sanction of the Government of the Republic is established by a regulation of the Government of the Republic, which establishes restrictions to the specific subject of the sanction.

2.3.4. The application of a financial sanction must be based on the UN Security Council resolution, an EU regulation or a regulation of the Government of the Republic.

2.3.5. In the event of requirements arising from the legislation, the provisions of the legislation on the sanction must be followed. In case of conflict with the legislation, the meaning and content of the ISA and the directly related legislation must be followed. Legislation and source materials[2] in English, which are directly related to the ISA must be based on their original wording and meaning.

2.3.6. The terms and definitions used in the Guidelines are defined in the ISA, the legislation implementing the international sanction, the Financial Action Task Force (FATF) 2012 Recommendations[3] and the 2013 methodology dictionaries[4] or the EU guidelines[5] and other guidance material.

2.3.7. For the purposes of the Guidelines, compliance with the requirements for the implementation and application of an international sanction means all the activities that the EU, the UN and the FATF request from the Member States and the persons having specific obligations when applying preventive measures.

2.3.8. When applying the Guidelines, the requirements arising from the legislation in force, international practice and the legislation directly related to the ISA, other advisory guidelines of Finantsinspektsioon, FATF and the Council of the European Union and other instruction materials[6] must be taken into account.

2.3.9. The principle of proportionality must be followed when implementing the Guidelines. This means that a person having specific obligations must draw up its own rules of procedure and internal control, apply the due diligence measures of the sanction and choose the means according to the nature, scale and sophistication of its company's economic activity, including risk appetite and risks associated with the activities of the person having specific obligations.

2.3.10. A risk-based approach must be taken into account when following the Guidelines. A person having specific obligations must first assess the risks associated with its own activities in order to plan, develop, and maintain a risk mitigation and risk management system of international sanctions corresponding to its ability, risk appetite and operational risks, considering that a risk-based approach does not release the person having specific obligations from the application of the sanction.

2.3.11. In the event of problems related to the implementation and interpretation of the Guidelines, the principle of reasonableness must be followed, interpreting, if necessary, the various points of the Guidelines in conjunction with each other and, considering the purpose of the Guidelines. It is also necessary to act in good faith and in accordance with the diligence expected of a person having specific obligations.

2.4. Terms and definitions

[2] Including legislation implementing an international sanction.
[3] The FATF Recommendations (2012). Available online at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf. (04/01/2021)
[4] The FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems (2013). Available online at: https://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf. (04/01/2021)
[5] Guidance and best practices. Available online at: https://www.consilium.europa.eu/en/policies/sanctions/. (04/01/2021)
[6] Including arising from general instruction materials on the organisation and activities of financial institutions.

2.4.1. An international sanction or a sanction of the Government of the Republic[7] is a measure of foreign policy, established by the EU, the UN or the Government of the Republic. It is a non-military measure implemented with the aim of maintaining or restoring peace, preventing conflicts and strengthening international security, supporting and strengthening democracy, and following the rule of law, human rights and international law. The measures can be (1) *non-economic* and (2) *economic*. Economic measures can in turn be divided into *(a) international financial sanctions and (b) trade sanctions.*

2.4.2. The subject of international sanctions is any natural or legal person, entity or body, designated in the legal act imposing or implementing international sanctions, with regard to which the international sanctions apply. The subject of international sanctions may also be a state, territory, territorial unit, regime, organisation, association, group or another unit, with regard to which the sanctions apply and who is identified as a subject in the legislation establishing or implementing the international sanction.

2.4.3. International financial sanction (the so-called sub-category of the economic sanction) is in particular a targeted measure directed against specific individuals or countries/regions. At the same time, financial sanctions are broadly divided into sanctions for terrorist financing and the financing of the proliferation of weapons of mass destruction and sanctions with other political content and purpose. The content of a financial sanction is to prohibit or restrict any move, transfer, alteration, use of or dealing with funds in any way that would result in any change in their volume, amount, location, ownership, possession, character or purpose or other change that would enable the use of the funds. The content of a financial sanction is also to prohibit any use of economic resources (assets of every kind, which are not funds but can be used to obtain funds, goods or services) to obtain funds, goods or services in any way, including, but not limited to, by selling, hiring or mortgaging them. Financial sanctions can be divided into two: *(i) a targeted financial sanction based on individuals* and *entities and (ii) an activity-based restriction on financing.* Detailed measures of the international financial sanctions, what and against whom these must be applied, are described in the legislation establishing or implementing the international sanction.

2.4.3.1. Targeted financial sanction[8] is established against an individual or a unit and refers to (a) the freezing of funds and economic resources, (b) prohibition on making funds and economic resources available, or (c) prohibition of the use of the financial system by the individual or entity included in the international sanctions list.

2.4.3.2. Activity-based restriction on financing refers to the prohibition of activities, such as the provision of financial assistance (funding, financing, including investing, conclusion of an insurance contract, securities transactions and lending) and other restrictions arising from the EU and the UN resolutions where the credit and financial institutions apply due diligence measures and apply restrictions and prohibitions during their activities, including when clearing funds.[9]

[7] In the EU terminology also 'restrictive measure'.
[8] Targeted financial sanctions, or TFS.
[9] Clearing refers to all activities related to the transaction from the giving of the order to the settlement.

2.4.4. **Financing of the proliferation of weapons of mass destruction** means any act for the provision of funds or financial services, used, in whole or in part, for the production, acquisition, possession, development, export, transhipment, intermediation, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their carriers and related materials (including technologies as well as dual-use goods used for illegal purposes), contrary to national laws or, where applicable, international obligations.[10]

3. Risk mitigation and risk management system of international sanctions

3.1. Strategy

3.1.1. The general strategy for the mitigation and management of risks of international sanctions describes the general guiding principles by which a person having specific obligations ensures that its activities are consistent with its risk appetite. The general strategy for the mitigation and management of risks of international sanctions may be contained in the risk appetite of a person having specific obligations.

3.1.2. Where appropriate, the strategy for the mitigation and management of risks of international sanctions shall be reviewed and updated and supplemented, including when the risk assessment or risk appetite is updated and supplemented, or when new sanctioning regimes are added.

3.2. Risk assessment and risk appetite

3.2.1. A person having specific obligations shall regularly prepare and update the risk appetite and risk assessment related to financial sanctions and financing of the proliferation of weapons of mass destruction, taking into account the principles set out in clauses 3.2 and 3.3 of the AML Advisory Guidelines of Finantsinspektsioon and the exceptions provided in the Guidelines.

3.2.2. The risk of financing a financial sanction and the proliferation of weapons of mass destruction includes not only the direct violation of a financial sanction, such as failure to freeze the sanctioned person's financial assets, but also the circumvention of the financial sanction. This principle must also be followed by the person having specific obligations when identifying, assessing, and analysing the risks.

3.2.3. Within the framework of the risk assessment of financial sanctions, the risk factors characteristic of financial sanctions must also be analysed for specific risk categories within the meaning of clause 3.3.4.1 of the AML Advisory Guidelines of Finantsinspektsioon, such as:

[10] The concept of financing the proliferation of weapons of mass destruction has been used more widely in the Guidelines, as there is currently no internationally agreed definition of financing the proliferation of weapons of mass destruction suitable for all regimes. This definition is based on the FATF report 'Combating proliferation financing: A status report on policy development and consultation' (2010). Available online at: https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf. (04/01/2020)

3.2.3.1. Client-related risks. Client risk refers to potential clients or client categories, whose activities involve higher risk of financial sanctions. One characteristic is the sophistication of the ownership and/or management structure; i.e. how easy or difficult it is to identify managers and beneficial owners, including owners. In case of the ownership structure, the risks associated with the client-managed or client-owned companies are also important (for example, if the client is the beneficial owner of the sanctioned company). This means that a person having specific obligations shall assess with enhanced due diligence clients, whose ownership structure is sophisticated or is otherwise risky. For risks related to clients, one must also take into account the risks related to the clients' business, i.e. the field of activity and the products and services offered, as well as geographical risks, such as the client's origin, habitual residence, place of registration and place of business.

3.2.3.2. Product, service, and transaction risks. Product, service, and transaction risks are related to the products and services offered by a person having specific obligations that are associated with a high risk of sanction or which products and services a client may use to circumvent the sanction. For example, the extent to which a person having specific obligations carries out cross-border transactions; how many and in which countries they have cross-border correspondent bank accounts; whether they offer products related to trade financing, payable-through accounts, virtual currency exchange, holding, transfer services, etc., correspondent banking services, etc.Online products and services may pose greater risks due to the speed of processing payments and the anonymity of access to the account, which means that this risk category is also exposed to the risks associated with the transmission channels of services.

3.2.3.3. Transmission channel risk. Transmission channel risk is related to the channels of receiving the service and products which the client uses both in establishing a business relationship as well as in the course of a business relationship, but also to the channels used by the person having specific obligations to sell its products and services. The above includes, in terms of the risk of financial sanction, in particular the risk that the products and services are consumable anonymously, which is why the person having specific obligations is unable to identify the location of the consumer of the service (for example, masking of IP addresses or consuming the service through intermediaries or representatives, including via lawyers/attorneys). A situation, where the client uses a broker or agent for communicating the person having specific obligations is also risky. It is also important to assess the risks associated with the transmission channels when relying on the due diligence measures applied by a third party service provider or, when a due diligence obligation has been outsourced, especially if such service provider is located in a jurisdiction with lower international compliance standards according to international assessments. Other channels used for providing the services, such as online banking and its availability, must also be assessed.

3.2.3.4. Geographical risks. Geographical risk relates to the exposure of the client, the products and services offered and the transmission channels of a person having specific obligations to certain higher risk jurisdictions. For this risk category, it is important, first of all, to take into account the risks associated with the country of location of the person having specific obligations and the risks arising from the geographical, cultural and historical links between its country of location and the country subject to sanctions. However, also situations, where the transactions are directly or indirectly related to a specific country or region with high risk of sanction, must be taken into account. For this risk category, also the countries and regions through which the sanction may be circumvented must be taken into account in addition to the countries and regions against which sanctions have been established. In the context of geographical risk, it is important to understand any indirect risks that may additionally arise if a transaction involves a high sanction risk (such as a product supply chain). As a result of the geographical risk assessment, the person having specific obligations determines which sanction lists should be screened for all jurisdictions and whether and which lists should be screened for certain jurisdiction(s).

3.2.3.5. With the systems used to identify the subject of a financial sanction, including technology-related risks if a person having specific obligations uses an automated screening tool (AST) of the financial sanction, when applying due diligence measures, they will evaluate the risks associated with the capability and manipulation of the technology. This is a separate risk category apart from the four usual risk categories.

3.2.4. The sanction risks faced by a person having specific obligations shall be determined on the basis of a methodology similar to that used in analysing the money laundering and terrorist financing risk, assessing the following:

- risk inherent to a person having specific obligations – the risk of sanction to which an authority is exposed without risk management and mitigation measures of sanction;
- efficiency of the risk management and mitigation measures of sanction;
- amount of residual risk (assessing the inherent risk and efficiency of mitigation measures).

3.2.5. The following formula shall be used for determining the risk characteristic of a sanction specific to a person having specific obligations:

inherent risk – efficiency of the risk management and mitigation measures of sanction = residual risk

3.2.6. A person having specific obligations must assess separately the risks of money laundering, terrorist financing and the financial sanction, including proliferation of weapons of mass destruction, by preparing a risk assessment. Risk assessments may be in a single document, but different risks must be assessed separately.

3.2.7. A person having specific obligations determines the risk appetite on the basis of the risk assessment. Risk appetite shall be subject to the provisions of clause 3.2 of the AML Advisory Guidelines of Finantsinspektsioon. The risk appetite of a person having specific obligations may also be described in the strategy for the mitigation and management of risks of international sanctions.

3.2.8. As a result of the risk assessment and risk appetite, the person having specific obligations shall establish a risk mitigation and risk management system of international sanctions for mitigating and managing risks. As in the event of risk assessment, the risk mitigation and the establishment of a risk management system must also take into account the possibility of circumventing the financial sanction and the management of that risk, in addition to the risk of breaching a financial sanction.

3.2.9. The risk mitigation and risk management system of international sanctions must be described in writing and shall include, *inter alia*, (i) the risk mitigation and risk management strategy (clause 3.1 of the Guidelines); (ii) the establishment and updating of the risk appetite and risk assessment (clauses 3.2 and 3.2.7 of the Guidelines); (iii) the rules of procedure describing the risk management and mitigation (clause 3.3 of the Guidelines); (iv) designation of the responsible persons and determination of their responsibilities (clause 3.4 of the Guidelines); (v) implementation of an appropriate training programme (clause 3.5 of the Guidelines); (vi) control measures to be implemented for the management of the risk, including the due diligence measures to be implemented (clause e3.6 of the Guidelines); (vii) the application of the financial sanction (clause 3.7 of the Guidelines); (viii) compliance with the notification obligation (clause 3.8 of the Guidelines), (ix) internal control instructions (clause 3.9 of the Guidelines) and (x) retention of data (clause 3.10 of the Guidelines). These measures are designed for the application and identification of the financial sanction measures in order to prevent circumvention of financial sanctions and avoid violations.

3.2.10. The risk mitigation and risk management system of international sanctions defines the principles and rules for identifying high-risk transactions, products, services, clients and geographical areas by a person having specific obligations. The risk mitigation and risk management system is proportionate and takes into account the practical needs, the nature, scope and sophistication of the economic or professional activities of the person having specific obligations.

3.2.11. The risk mitigation and risk management system of international sanctions shall be clear and easy to understand, provide a clear overview for the whole organisation and define the roles and responsibilities. The system includes standards and requirements, which must be complied with.

3.2.12. The risk mitigation and risk management system of international sanctions contains rules of procedure and internal control that provide guidance on the identification of the subject of financial sanction, the application of financial sanction, including for the retention and reporting of frozen funds, and control measures to mitigate or manage the risks arising from the financial sanction. Among other things, the risk mitigation and risk management system of international sanctions provides an overview and guidance on how to act in a situation, where a subject of the financial sanction, a higher risk or an indication of danger is identified. It shall include a description of the actions taken by a person having specific obligations in order to reach a decision to impose the measures of financial sanctions, to refuse a transaction or a service.

3.3. Rules of procedure

3.3.1. The rules of procedure and guidelines for international financial sanctions describe the principles and activities for the application and identification of financial sanctions. The rules of procedure define the policy on how to control the client base and the transactions carried out by the person having specific obligations and to identify the subject of the financial sanction.

3.3.2. The rules of procedure shall correspond to the practical needs of the person having specific obligations, the nature, scope and degree of sophistication of its economic or professional activities, including the risk appetite and the risks associated with the activities of the person having specific obligations and shall be in writing or in a form that can be reproduced in writing.

3.3.3. The person having specific obligations shall establish the rules of procedure to effectively mitigate and manage the financial sanctions and the risks associated with the financing of proliferation of weapons of mass destruction and to ensure an organisational structure that allows for the immediate detection of the entry into force, amendment or termination of a financial sanction. The rules of procedure of a person having specific obligations shall contain at least the following instructions:

3.3.3.1. on the identification of the subject of the international financial sanction and the transaction or act in breach of the financial sanction;

3.3.3.2. on how to act in the event of identifying the subject of the international financial sanction and a transaction or act in breach of the financial sanction;

3.3.3.3. on the identification of the risk of breach of international financial sanctions and upon such identification on how to act, including the procedure for identifying and investigating possible breaches or circumvention of financial sanctions, including the procedure for timely identification of the risk of financial sanctions and financing of the proliferation of weapons of mass destruction before the transaction, an occasional transaction, before the establishment of a business relationship and throughout the validity of the business relationship;

3.3.3.4. upon the application of due diligence measures on the collection of additional information, including when to request additional information from a partner or client and how to retain the collected data;

3.3.3.5. on the compliance with the notification obligation set out in clause 3.8 of the Guidelines;

3.3.3.6. on the retention and making available of the data set out in clause 3.10 of the Guidelines.

3.3.4. With the rules of procedure, the person having specific obligations shall define the responsible persons and their duties and competencies.

3.3.5. The rules of procedure regulate the flow of information within the company regarding financial sanctions and the financing of the proliferation of weapons of mass destruction.

3.3.6. The person having specific obligations introduces the rules of procedure, instructions, etc. to all its employees whose duties include establishment of a business relationship, monitoring or concluding transactions.

3.3.7. The rules of procedure are reviewed on a regular basis and updated, if necessary.

3.4. Appointment of management board member in charge and a responsible person and the responsibility of the management

3.4.1. For the purposes of the Guidelines, section 17 of the Money Laundering and terrorist Financing Prevention Act (hereinafter the *MLTFPA*) and clause 3.4 of the AML Advisory Guidelines of Finantsinspektsioon apply to the responsibility of the management board and appointment of management board member in charge.

3.4.2. A person having specific obligations shall appoint a person responsible for the performance of the duties provided for in the ISA and the Guidelines, including the application of a financial sanction (hereinafter *responsible person*) and shall forward his or her contact details to the Financial Intelligence Unit and Finantsinspektsioon. A person having specific obligations shall notify the Financial Intelligence Unit and Finantsinspektsioon in writing within 30 days of the appointment of the responsible person or their substitute and the details of the person.

3.4.3. Section 17 of the MLTFPA and the provisions of clause 3.5.3 of the AML Advisory Guidelines of Finantsinspektsioon shall apply when appointing a person responsible for the person having specific obligations and in respect of the duties and rights of the responsible person, taking into account the features specific to the implementation and application of the sanction.

3.4.4. The person having specific obligations shall ensure that the responsible person has sufficient skills and knowledge to perform the duties of application of the financial sanction and to make a decision on lawful action.

3.4.5. The responsible person shall be responsible for compliance with the regulatory provisions established in the field of financial sanctions and for taking the measures arising from financial sanctions, as well as for reporting actual or possible violations of the sanctions.

3.4.6. The person having specific obligations shall ensure that the person responsible for the application of the financial sanction has sufficient authority and access to the information necessary for the performance of his or her duties.

3.5. Training of employees

3.5.1. Training is one of the most important ways of raising awareness of the obligations involved in the application of international sanctions. Training, including knowledge of international sanctions, typologies, means of circumvention and obligations, is necessary so that the employees know what to do when they are exposed to a possible breach of an international sanction. Training helps to mitigate the risks associated with the application of international sanctions that a person having specific obligations may face. Training must correspond to the specificities of the authority, i.e. take into account the products and services offered, the clients, partners and the geographical area in which it operates and comply with the principle of proportionality.

3.5.2. A person having specific obligations shall ensure that its employees, whose duties include the establishment of business relationships or conclusion of transactions, are trained in the fulfilment of obligations arising from the ISA and the legislation implementing international sanctions.

3.5.3. For the purposes of the Guidelines, the provisions of clause 3.7 of the AML Advisory Guidelines of Finantsinspektsioon shall apply to the training of employees, taking into account the specificity of financial sanctions.

3.6. Due diligence measures for the identification of financial sanctions

3.6.1. A person having specific obligations shall establish a process for controlling the subject of the financial sanction and determining the risk level of the sanction with respect to the existing clients and the establishment of new client relationships. Such a solution is based on the sanction lists, obligations, and restrictions arising from sanction regimes, the application of standard due diligence measures under the MLTFPA and the specific due diligence measures of the financial sanctions, such as screening, and the data collected in the course of an independent investigation by a person having specific obligations.

3.6.2. A person having specific obligations shall ensure the use and updating of the client data in the course of the business relationship, including in the control of the client's transactions, to exclude the breach of the financial sanction and prevent the circumvention of the financial sanction.

3.6.3. A person having specific obligations shall apply the due diligence measures of financial sanctions:

3.6.3.1. upon the establishment of business relationships;

3.6.3.2. in the course of business relationships;

3.6.3.3. in carrying out transactions;

3.6.3.4. in the event of a risk of breach or suspected breach of a financial sanction.

3.6.4. A due diligence measure of the financial sanctions specified in clause 3.6.3 of the Guidelines is collecting additional information on:

a. whether the person with whom it has a business relationship or who intends to enter into it is the subject of a financial sanction;
b. whether the planned or performed transaction or act breaches the financial sanction;
c. the purpose and nature of a business relationship, transaction or act.

3.6.5. A person having specific obligations shall verify the obtained additional information on the basis of additional documents, data or information from a reliable and independent source.

3.6.6. When deciding on the scope of the due diligence measures of the sanction, it is important to assess all the aspects related to the risks, including the client risk, the risk of products and services offered by a person having specific obligations, sales channel risk and geographical risks, and how these risks are mitigated. When assessing the geographical risk it is important to understand the geographical market share of the client. The due diligence measures applied by a person having specific obligations shall be proportionate and shall take into account the risks of sanction arising from its business.

3.6.7. The data collected in the course of due diligence must be relevant and up-to-date, taking into account that financial sanctions change over time. Continuous timing and updating of due diligence measures is necessary to ensure the screening of the client and transactions (before the transaction is made) in order to prevent a breach of the financial sanction.

3.6.8. A person having specific obligations shall determine the manner and means to check whether the client or a person or an entity related to him is subject to a financial sanction and that the execution of transactions would not violate the financial sanction. These means may be manual systems as well as an automated screening tool (AST).

3.6.9. If a person having specific obligations decides to use AST in its screening system, then Annex 1 to the Guidelines 'Automated Screening Tool' shall apply to it, including the person will take into account the principles of proportional approach in Annex 1.

3.6.10. The means used must be risk-based and proportionate, i.e. they must correspond to the size of the person having specific obligations and the nature, scope, level of sophistication of the activities and products and services offered, including the risk appetite and risks in the business of the person having specific obligations. This means that the larger is the client base of the person having specific obligations (person having specific obligations is unable to manually monitor the clients and transactions) and/or the more transactions, including in particular high-risk transactions are made by the person having specific obligations, and the higher the risk of associated financial sanctions, the more or more funds or the more extensive funds must be used by the person having specific obligations to identify the situation or risk of a financial sanction. More extensive tools refer to automated and technological monitoring and screening programs, their scope, capabilities, effectiveness, etc. A person having specific obligations performs manual screening in cases where the risk is low or there are only few transactions or clients[11], or where comparable data cannot be found from reliable sources in digital or other form required for automatic screening (e.g. from trade documents).

3.6.11. The person having specific obligations also monitors the media and uses the information collected in the company during the due diligence screening of clients and transactions and, if necessary, adds to the internal screening list (if such list exists) persons and entities identified as being at high risk of sanctions or high risk in relation to the financing of the proliferation of weapons of mass destruction.

3.6.12. A person having specific obligations shall know its client. A sophisticated (ownership) structure creates additional links between the persons in control of the company or activities and the person having specific obligations. This creates opacity and prevents a person having specific obligations from understanding the content, purpose and actual persons involved in the transaction, incl., whether it is the subject of a financial sanction or a person under its control, or whether the transaction violates the financial sanction. The sophistication of the company's (ownership) structure is assessed through the application of due diligence measures based on the pre-defined rules of procedure of the obligated person. Assessment, together with the relevant criteria, must be documented.

3.6.13. The person having specific obligations shall define internal control rules and ensure that the lists of subjects of the sanctions that it uses are accurate, reliable, up-to-date, constantly updated and proportionate to the risks managed by the person having specific obligations.

3.7. Application of financial sanctions

3.7.1. A person having specific obligations shall apply the financial sanctions pursuant to as provided in the legislation implementing the same.

3.7.2. A person having specific obligations shall apply financial sanctions if:

3.7.2.1. they identify the subject of the targeted financial sanction;

3.7.2.2. the planned or performed transaction or act breaches the financial sanction;

3.7.2.3. they doubt whether the person with whom it has a business relationship or who intends to enter into it is the subject of a targeted financial sanction;

3.7.2.4. they doubt whether the planned or performed transaction or act breaches the financial sanction;

[11] Considering the clients, transaction volume or sophistication and the resources in use.

3.7.2.5. after application of the due diligence measures, it is not possible to determine whether the person who has or intends to have a business relationship with them is the subject of a targeted financial sanction or whether the person who intends to conduct an occasional transaction violates the financial sanction.

3.7.3. If a subject of a financial sanction has a minority interest in an entity, this does not necessarily mean that it is not subject to a financial sanction. In this case, the person having specific obligations shall apply additional due diligence measures, to check whether the subject of financial sanction has a control over the entity.

3.7.4. A person having specific obligations shall freeze the funds and economic resources of the subject of a targeted financial sanction, even if these are jointly owned by several persons. The definition of joint ownership is based on the law governing ownership relations, established in Estonia. Thus, for the purposes of the ISA, joint ownership is the ownership of two or more persons in unspecified parts in a common matter at the same time.

3.7.5. Funds and economic resources jointly owned by a person or entity who is not the target of the freezing measures of funds and economic resources of a subject of targeted financial sanction shall, in practice, be frozen as a whole. This means that in the event of a freezing of assets, the own funds and economic resources of the person entered in the sanctions list must be included, even if these are jointly owned with another person or if the person entered in the sanctions list owns only part of these. In addition, the own funds and economic resources of a person entered in the sanctions list are considered to include any interests (whether legal or otherwise) that belong to him. The above also applies if two or more persons jointly hold shares, units or rights. The same principle applies to joint agreements, where all holders of shares, units or rights exercise their rights jointly. The above must be taken into account when assessing the person's holding or voting right in an entity.

3.7.6. The freezing of assets shall not affect funds and economic resources which do not belong to the subject of a targeted financial sanction, the owner of which it is not and which are not under its control. Therefore, the freezing of funds does not concern the funds and economic resources of an entity which is a separate legal entity of a subject of targeted financial sanction and which is not the target of the measures, unless these are owned or controlled by the subject of the targeted financial sanction.

3.7.7. A person having specific obligations shall follow the guidelines[12] in chapter K, item I of the EU Sanctions Guidelines when assessing whether another person or entity controls a legal person or entity, including on their own or under an agreement with another shareholder or third party.

3.7.8. A person having specific obligations shall follow the guidance set out in chapter K, item II of the EU Sanctions Guidelines[13] when assessing whether there may be a situation where the funds or economic resources are made available indirectly to persons and entities entered in the sanctions list.

3.8. Notifying the Financial Intelligence Unit

3.8.1. A person having specific obligations shall notify the Financial Intelligence Unit, including of the applied measures of financial sanctions if they have:

[12]Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy, https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf.
[13]Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy, https://data.consilium.europa.eu/doc/document/ST-5664-2018-INIT/en/pdf.

3.8.1.1. identified the subject of a targeted financial sanction who is in or plans to establish a business relationship;

3.8.1.2. applied financial sanctions;

3.8.1.3. identified a planned or actual transaction in breach of the financial sanctions;

3.8.1.4. identified breach of financial sanctions, including circumvention;

3.8.1.5. there is a suspicion of a possible breach or circumvention of an international sanction and the due diligence has not removed the suspicion.

3.8.2. Before applying a financial sanction and submitting a notification to the Financial Intelligence Unit, a person having specific obligations must take reasonable steps to ensure that the identified person is entered in the sanctions list (i.e. by also checking other identifiable information)[14]. In case of suspicion of a prohibited transaction or a subject of a financial sanction, the person having specific obligations shall collect information on the transaction, taking into account the principle of reasonability. Additional information that is useful for identifying sanctioned persons and entities is provided by data in both the UN[15] and EU sanctions lists. These may include the person's full name, date and place of birth, nationality, residence, pseudonym and a reason for inclusion in the list. Also INTERPOL publishes special notices on certain persons entered in the list,[16] which may include photos.

3.9. Rules of internal control

3.9.1. The rules of internal control are an internal procedure for verifying compliance with the rules of procedure, etc., including AST-testing if used by a person having specific obligations. The rules of internal control describe, *inter alia*, the frequency of internal control, the procedure for conducting internal control and the procedure for retaining the results.

3.9.2. The rules of internal control must cover the verification of the means used by the employees and the person having specific obligations. This ensures, *inter alia*, that the system for monitoring compliance with the financial sanctions functions as intended and within the set parameters.

3.9.3. The rules of internal control shall describe the functioning of internal control, incl. including, where appropriate, the procedure for applying internal audit and compliance. Among other things, it must be specified who, how and how often verifies the compliance of the person having specific obligations with the requirements of the employees, systems, rules of procedure, etc. The rules of internal control must be described in sufficient detail to give the employee an understanding of who controls his or her line of work.

3.9.4. All controls and processes related to financial sanctions must be documented. A person having specific obligations shall prepare the control and supervision documents, including the procedures of handling suspicious cases. The timeliness and relevance of documents must be ensured.

[14] A person having specific obligations has taken sufficient reasonable steps if it has an internal conviction that it has complied with the due diligence obligation. The principle of reasonableness is taken into account in the formation of internal conviction. This means that when applying due diligence, the obligated person must have the knowledge, understanding and belief that sufficient data has been collected.

[15] *UN Security Council Narrative Summaries of Reasons for Listing* https://www.un.org/securitycouncil/sanctions/narrative-summaries .

[16] *INTERPOL–UN Security Council Special Notices* https://www.interpol.int/How-we-work/Notices/INTERPOL-United-Nations-Security-Council-Special-Notices.

3.9.5. It is also a good practice to introduce the results of the control to the employee and, if deficiencies are identified, to submit proposals to the management board in order to introduce the necessary changes to the risk identification and management system or the application of due diligence measures or other activities related to compliance with the ISA requirements.

3.10. Retention of data

3.10.1. A person having specific obligations collects and retains the data relating to (i) controls on whether a person who is in or plans to establish a business relationship with it is subject of a financial sanction; (ii) controls on whether a planned or performed transaction or act violates a financial sanction; (iii) the application of a financial sanction; and (iv) notification to the Financial Intelligence Unit. Data collected in the course of the implementation of due diligence measures must also be retained.

3.10.2. The data shall be stored, *inter alia*, in a way that allows an exhaustive and immediate response to the requests of supervisory authorities or other persons entitled to do so.

3.10.3. The data arising from clause 3.10.1 of the Guidelines (except for clause (iv)) must be retained for five years after the termination of the business relationship or the occasionally performed transaction. Data relating to compliance with the notification obligation pursuant to clause iv shall be retained for five years after compliance with the notification obligation.

3.10.4. If a person having specific obligations makes an inquiry to the national electronic database for the application of due diligence measures, the data retention obligations shall be deemed to be fulfilled if the information on making the electronic inquiry to the register is reproducible within five years after the termination of the business relationship or performing an occasional transaction.

4. Implementation of the Guidelines

The Guidelines are valid from 01/02/2022. As the Guidelines clarify the applicable law, these do not change the validity of the requirements arising from the legislation. Different explanations of the Guidelines may also be immediately valid if it is a relevant and recognised professional standard in the financial sector the knowledge and implementation of which can be expected from a person having specific obligations.

Annex 1 – Automated Screening Tool

For larger and more sophisticated financial institutions, it is assumed that the screening system uses technology as a certain key function to ensure the creation and management of appropriate alerts. Such functions include the ability to apply risk-based screening rules. This Annex describes the internationally accepted principles and expectations to AST, that has been integrated into the screening program. The information provided in this Annex may not be exhaustive, as modern technological development is rapid and the personal expectations of a person having specific obligations for AST may be different. If a person having specific obligations decides to use AST, it shall take into account the principle of proportionality set out in clause 3.6.1010 of the Guidelines.

Implementing the rules of screening technology

When implementing the rules of AST, the principle of exact matching or fuzzy logic is used. It is common and recommended to combine both rules. Screening technology may also use additional and restrictive rules, incl., whitelisting,[17] to which the data is entered on persons and entities previously identified as false matches and in which case it is not a subject of a financial sanction or a client or a transaction that would have a high risk of a sanction. Using such lists helps to reduce the number of false matches. The whitelist is evaluated and updated periodically and when risk factors emerge for any person or entity entered in the list.

With regard to screening technology, a person having specific obligations shall set a screening threshold in AST that corresponds to the risks and risk appetite arising from its activities. In order to define a correct and fair screening threshold, a person having specific obligations must understand AST and be aware of the authority's higher risks of financial sanctions and financing the proliferation of weapons of mass destruction. The screening threshold is also determined by the quality of the data and the control that the person having specific obligations has over the data being screened. Where a person having specific obligations is aware of the deficiencies in the quality of the data of financial institutions related to itself or a counterparty, the screening threshold shall be lowered accordingly.

When applying the screening rules in AST, it must be borne in mind that some data are in different formats and presented differently. Transactions containing such data may require manual review processes where the relevant information is manually verified. Good screening quality in AST is ensured by high-quality client and transaction data used for screening, which is, among other things, clean or purified. High-quality data ensures easier and more effective control against sanction lists.

A review and updating of the algorithms and screening thresholds used by AST shall be performed when new patterns, typologies, high-risk factors, false negative matches are identified, or when new sanction regimes change and are added.

When using AST, a person having specific obligations shall establish the transliteration and transcription rules to ensure that personal and place names are unambiguously identifiable and that the spelling is comparable to the indicators in the sanctions lists.

Ensuring relevance of AST

A person having specific obligations shall ensure that updates, changes (addings to the list, delistings and changes in the relevant details of the subject of sanction) in the AST are updated and implemented without delay with reasonable effort.[18] in order to ensure this, the person having specific obligations shall determine which updated data on the sanction, published by the competent authorities, shall be monitored by the

.

[18] According to the FATF interpretation, the funds of a subject of a targeted financial sanction are frozen without delay, ideally within a few hours after the person or entity is entered in the sanctions list. The updating of the lists must be based on the principles of reasonableness and best effort, i.e., the person having specific obligations makes reasonable efforts to keep the sanctions lists relevant and up to date.

employees and the adequate frequency of verifying such updates. The person having specific obligations shall also define the competent persons who may make changes to the lists and shall ensure that only competent employees authorised to do so can add or remove lists or list entries.

The sanctions lists used by a person having specific obligations for screening also include information published by the competent authorities establishing the sanction as well as the information collected personally by the person having specific obligations on the basis of know-your-customer principles, which will help it to better identify the subject of the sanction, the transaction infringing the sanction or the high risk of sanction.

Listings prepared by third parties may also be used for screening if (i) in the event of outsourcing, compliance with the rules for outsourcing the activities set out in the Advisory Guidelines of Finantsinspektsioon 'Outsourcing Requirements for Supervised Entities'[19] is guaranteed, (ii) also, if it has been ensured that the legally binding sanctions lists are accurate and updated without delay, and finally (iii) the person having specific obligations has made reasonable efforts using its best professional skills to assess the quality of the service in question.

Screening technology requires continuous calibration, validation and improvement to ensure efficient screening of data. To this end, the person having specific obligations shall establish and implement an internal control system to prevent the stripping,[20] alteration and other manipulation of relevant data, both internally and externally. At the same time, higher attention should be paid to the part of the transaction process where a client or an employee of an authority is able to manipulate the information used in screening.

When screening the client data in AST, appropriate independence of controls from risk assessment and client risk should be ensured.

A person having specific obligations shall ensure that all results of screening, technology, system calibrations, alterations, updating and testing are documented and stored.

Evaluation of alerts arising from screening technology

Each alert created by AST and its matches must be evaluated and a final decision made. For transactions involving high risk of financial sanctions or the financing of the proliferation of weapons of mass destruction, it is recommended to use the four-eyes-principle in the decision-making process[21].

A person having specific obligations shall document the results of the monitoring and screening of the client and transactions, incl. the false and true matches and the data, on the basis of which the decision was reached. Through this activity, it is possible to analyse the results of screening and provide the management with a report on the effectiveness, trends, typologies and functioning of the monitoring and screening system.

Measures to be implemented in parallel with screening technology

A person having specific obligations shall take into account that automatic screening alone is not a sufficient due diligence measure to mitigate the risks of financial sanctions, including financing the proliferation of weapons of mass destruction, risk management and the prevention of violations. Therefore, a person having

[19] Advisory Guidelines of Finantsinspektsioon 'Outsourcing Requirements for Supervised Entities'. Available online at: https://www.fi.ee/sites/default/files/2019-08/pp%20nr%2004%2005.08.2019%20Tegevuse%20edasiandmise%20FI%20juhend%20uues%20redaktsioonis%20ET_0.pdf. (04/01/2021)

.

[21] The four-eyes-principle is a requirement that two people must reach an agreement before performing operations. The four-eyes-principle is sometimes called the two-man-rule.

specific obligations must apply to clients and transactions with a high risk of financial sanction also other and broader due diligence measures, such as client and transaction risk analysis.

In the event that a person having specific obligations decides to use the outsourced service in the case of a monitoring or screening system, including the ATS, the requirements applicable to the outsourcing of activities specified in the Advisory Guidelines of Finantsinspektsioon 'Outsourcing Requirements for Supervised Entities'[22] and the responsibility for the outsourced service and processes that ensure compliance in the application of the financial sanction shall remain to the person having specific obligations shall apply.

In the event of services outsourced to comply with AST or other legal acts or guidelines, the activities and processes must be documented, including the activities of the subcontracting company, regular testing and inspections. In the event of large-scale subcontracting, the termination or prevention of the termination of a subcontracting contract must be defined in order to ensure the consistency and quality of the outsourced activities and processes.

A person having specific obligations (correspondent institution) mediating the transactions must use reasonable solutions to identify high-risk transactions where there is no information on the originator or beneficiary. Such measures should be in line with the principles of processing payments and the Regulation (EU) 2015/847 of the European Parliament and of the Council.

Testing

When a person having specific obligations uses AST to control sanctions, it shall conduct regular and need-based tests to verify its effective functioning and to manage and mitigate the risks identified with the risk assessment.

AST testing shall be supported by indicators, analysis and reporting that enable to identify the occurrence of financial sanctions, technology and operational risks and the risks arising from data quality.

A comprehensive, independent and objective testing or audit function ensures that the person having specific obligations is aware of where and how their systems work and when they should be upgraded, supplemented or reconfigured to meet the risk assessment and indicators of sanction regimes.

To apply the above, the person having specific obligations shall:

- ensure that the person conducting the test or audit is impartial, independent and has sufficient authority, skills, experience and resources to do so;

- ensure that if the outcome of a test or audit is not as expected, effective measures are taken without delay to identify and implement compensatory measures until the root cause of the system's weakness can be identified and risks mitigated and managed;

- document the structure of its AST so that it is clear whether the risks associated with the activities of the person having specific obligations have been identified and managed, including the transparency of the system's bottlenecks and other measures is demonstrated (e.g. the risks are mitigated by other due diligence measures);

- implement an independent risk-based testing system to ensure that AST generates appropriate and high-quality alerts, including matches corresponding to the risk appetite.

[22] Advisory Guidelines of Finantsinspektsioon 'Outsourcing Requirements for Supervised Entities'. Available online at: https://www.fi.ee/failid/Nouded_finantsjarelevalve_subjekti_poolt_tegevuse_edasiandmisele_outsourcing_v6.pdf. (04/01/2021)

Independent testing shall be carried out by qualified employees with the relevant technological experience or by independent employees of the compliance department of a person having specific obligations or by a third party acting for that purpose or a combination thereof.

The testing may include, but is not limited to, at least the following:

- Exact match – the tested full name is compared against the list. In this way, not only the process of generating matches is tested, but also the dataflow is tested to ensure that a match is obtained for all data sources;

- Phonetic similarity – names that sound similar (such as Graig or Greig) are tested;

- Missing or added characters – tests are conducted when spaces, hyphens, symbols are added, or are removed. Such situations may arise, for example, when a name in a non-Latin alphabet is changed to a name in Latin alphabet. This need for testing is important to ensure that the IT system can detect differences in punctuation marks, missing components, or letters;

- Wrong data fields – a test is conducted on the generation of matches when data is entered in the wrong data fields or when data fields have changed during the transfer of data from one system to another;

- Spelling differences – it is tested whether there are differences in the same or similar names (such as Aleksey or Alexei);

- Titles or honorary titles – it is tested whether the systems recognise names when titles or honorary titles (such as Lord or Mr) are added to names;

- First and last name have been exchanged – a test is conducted if the first name and last name have been exchanged in the data;

- In different foreign languages – it is tested whether the system recognises the names in their native language (e.g. Jüri and Jyri);

- Recognition of alias, aka[23] – It is tested how the systems use the variations of aliases (nicknames). Do they identify aliases and how they are dealt with according to the risk appetite;

- Noise simulation – it is tested whether the systems detect a match when a character is added, replaced, or changed. For example, when letter O is replaced by character zero (0), etc.

A person having specific obligations shall analyse the test results and assess whether to accept or mitigate the detected deficiencies. If necessary, the employee verifying the test results shall propose additions or changes to the systems.

.

Annex 2 – Estonian-specific risks and methods associated with circumvention and infringement of sanctions

This Annex is based on various risk assessments, typologies, data available to Finantsinspektsioon, statistics and findings from on-site inspections, and specific information. It takes into account the services and products provided by financial institutions and their volume and the geographical position of Estonia.

Some of the characteristics listed in this Annex may occur individually or in together in normal or legitimate transactions; therefore, the provided non-exhaustive list should be considered as assistance in identifying the risks involved.

The following does not require a person having specific obligations to apply due diligence measures in all single cases and request additional information to identify potential risks. A person having specific obligations must make a decision on requesting additional information or a need for that in a proportionate and risk-based manner.

The subjects of financial sanctions rarely, if at all, appear among the parties to the transaction. Instead, they use sophisticated schemes and shell companies to hide their participation. The main violations and circumvention of financial sanctions are carried out with the help of third parties and intermediaries. It is therefore necessary for person having specific obligations to be aware of and keep up with the risks and typologies associated with financial sanctions and the financing of the proliferation of weapons of mass destruction.

This Annex sets out the risks inherent in financial sanctions and the methods of circumvention. Nevertheless, a person having specific obligations must also take into account the risks and methods related to money laundering and terrorist financing, which are further specified in the AML Advisory Guidelines of Finantsinspektsioon, as the risks related to money laundering and terrorist financing may be similar, incl. concealment of the beneficial owner and countries with a high risk of money laundering, terrorist financing and financial sanctions. Also the regions and countries with weak controls and laws to fight financial crime are similar. However, the risks and methods inherent in financial sanctions must be taken into account in the risks and methods associated with money laundering and terrorist financing.

It is important that the alerts cannot always be viewed alone and in isolation. Relevant alerts are viewed and assessed jointly with other alerts. The assessment of alerts must be based on the client, its activities and the area where the client operates or where the goods are purchased or sold.

The circumvention or violation of a sanction by manipulating the screening systems can take place in at least two ways.

External circumvention – a client or a third party related to the same breaches a financial sanction. This means that an outside party removes or fails to transmit important data related to the transaction. Such stripping or failure to transmit data is a desire to conceal the identity of the remitter, beneficiary or jurisdiction of the payment, as well as the origin or destination of the goods or services. Sanctioned persons may also use the accounts of family members or relatives.

Internal circumvention – the organisation's own employees commit a violation. For example, they remove important data related to a transaction or an employee fails to apply due diligence measures, e.g. they use clients' accounts to hide the origin of the funds.

Ways and risks of concealing identity:

Using different names:

- The remitter's or beneficiary's name is slightly changed or shortened, spaces are added to the name, or the middle name is omitted.

- An incorrect address is provided that differs from the address of the subject of sanction.

- The subject of the sanction may act using nominees, relatives, friends or close ones, making it more difficult to identify the person or entity.

- Using common words in the names by legal persons. The use of such names can make it difficult to identify a match, and the alert generated by AST can be ignored without further investigation.

Concealing the beneficial owner:

- It is difficult to identify the beneficial owners of companies with sophisticated ownership structures. Tracing the beneficial owners of such schemes is challenging when there are several legal entities in the ownership chain. Identifying the beneficial owner can also be difficult when there are companies in the ownership structure of the company that are established in a jurisdiction where it is difficult to obtain information on the beneficial owners. In essence, the (ownership) structure of a company must be described if its sophistication means that the company and its activities are not transparent to a person having specific obligations. This assessment may be based on, without limitation:
    - the number of associated companies in the structure;
    - the number of countries involved and their geographical risk;
    - economic justification of the structure;
    - the extent to which the information concerning the structure is available in official registers or publicly validated documents;

various risk-increasing and risk-reducing factors also play a role in risk assessment. For example, the following factors may reduce the risks:

- long-term business relationship with frequent client contact;
- a branch or representation in the relevant countries ('national desks') or, as appropriate, extensive experience (language skills as well as political, socio-cultural and regulatory background knowledge) in the countries concerned;
- involvement of countries of the EU/EEA or equivalent third countries.

In particular, the following risk-increasing factors shall be taken into account:

- the signature rights of the sole owner and general or special authorisations of third parties;
- structures established by third parties;
- involvement of countries with which the person having specific obligations has no experience;
- recently established business relationships;
- little contacts with client;
- unclear purpose or economically questionable structure at the request of the client;
- deviation from the client's previously known needs (see business profile), i.e. unusual and incomprehensible structuring.

It should be taken into account that the existence of a single criterion is generally not sufficient to assess the sophistication of a business relationship – a general view, taking into account all the relevant criteria, is decisive.

- With the help of bearer shares and bonds, it is possible to conceal the beneficial owners of the company. The documentation of these instruments does not indicate the beneficial owner. Theoretically, the owner of a company is the one who holds or who physically holds the certificate of the bearer shares or bonds.

- Dilution of the ownership of a sanctioned person may seem legal, but it still carries a high risk of sanction as the ownership structure may change again. Sophisticated ownership structures, where several

entities are located in different jurisdictions, may reduce the ownership of the subject of sanction below the 50% threshold so that entity is not subject to restrictions and the same sanction measures as the sanctioned person. An example of this is when a subject of sanction invests in companies, which in turn finance the companies of a non-sanctioned person. Those companies that are not subject to a sanction can trade legally, but the subject of sanction cannot. The network of subsidiaries, intermediaries and authorised representatives ensures that technically, there is no breach of the sanction. The result, however, is that the sanctioned entity is able to procure the resources and goods to which the sanction tries to deny access.

- The use of procurators, nominees, frontmen, where someone else acts as if they were the owner, having control over the funds or the company. In some cases, even if it is possible to obtain information on the company's data, these include only representatives or shareholders, but not beneficial owners.

- Transactions where the subject of sanction sells the holding to an associated company or a close person (family member, business partner, colleague or friend), refer to the ownership transfer scheme. Such transaction does not show that the subject of sanction owns the company, but the subject of sanction may still have control over the company's assets and decisions.

Manipulation of transaction data:

- It is important to pay attention to the entire control system. Despite the good technological tools and expertise, technology can be manipulated to exploit the system to violate or circumvent the sanction. For example, manipulation of the AST, where the data related to the transaction is transmitted in such a way that the identity of the sanctioned party cannot be established. Information that could be used to identify the parties has been removed or replaced, either by the client or by the employee himself or herself. This is one of the most common methods of circumventing sanctions. Data may be changed or removed without the knowledge of other participants in the transaction.

- Reorganisation of data, if they assume or know that certain data fields are not checked.

- Replacing data with false information. For example, the bank unique identifier of a bank in a country with a low risk of sanction is used.

- Use of unusual character combinations, such as '% &% $%'. Special characters are used that may appear as letters but cannot be recognised as letters by automatic filters (o and zero).

- An attempt is made to avoid identification by changing the name or submitting information in other fields that are 'Mandatory'.

- Explanations that appear as alerts, such as 'No Name' or 'On behalf of…' are used.

Alerts and risks associated with different payment channels:

- E-wallets and payment service providers may implement inadequate client identification controls, allowing the subjects of sanction to use their services anonymously. For example, to hide the identity of users, multiple e-wallet accounts can be accessed from a single mobile device. Some countries do not regulate the use of e-wallets and have not established requirements to help identify the subject of sanction. In this context, the subject of sanction may take advantage of the regulatory loopholes or a general incomprehension of the criminal methodology related to e-wallet technology.

- Prepaid cards, where they can be purchased without applying the same due diligence measures as for other payment cards. This, however, means that the users are not identified in the same way and the card provides anonymity. Many open prepaid cards can be used in global payment networks, facilitating funding in one country and cash withdrawals in another. Prepaid cards are physically similar to regular credit

cards and can be discretely transported in many environments as an alternative to large amounts of cash. The origin of the funds charged to the cards and the history of such transactions could be concealed.

- Virtual currencies are high risk due to their anonymity and incomplete end-user information, such as the data on the originator and beneficiary of the payment are encrypted or incomplete. These types of currencies pose challenges especially to sanction regimes and types of sanctions, such as financial sanctions, which are based on the data of the recipient and sender of the transaction.

- Use of *Hawala/Hundi* type systems to conceal the illegal origin of assets. Such schemes are primarily associated with the desire to conceal a high-risk region or area. *Hawala* may be used for the purpose of concealing the actual remitter or beneficiary and transactions involving illegal goods (drugs, precious metals, etc.).

- Use of *U-turn payment,* to conceal the initial origin (beneficiary) or high-risk jurisdiction of the funds.

Ways of infringement in connection with a jurisdiction and alerts

- The address refers to another nearby country or region. For example, in the case of a Crimea-related sanction, Russia or the Ukraine are entered as the address of the beneficiary or remitter.

- An important part of the address is omitted. For example, the name of the province is given, but the country is omitted or replaced by another country.

- A (shadow) company located in a nearby area is used.

- The entered address is an address that is similar to the address of the subject of sanction, with a slight difference. For example, the same street, city, country, but a different house number.

- The client's partner has a business in a country or region with a high sanction risk.

- The same address is shared with a subject of sanction.

Alerts of transactions related to activity-based restriction on financing and methods of circumvention:

- Concealment of identity. Provision of incorrect data on the consignee or consignor.

- It is concealed that these are restricted goods. The client does not want to provide information about the end-user of the goods.

- A shadow company or a letter-box company is used. The goods or services do not correspond to the business of the company. The company has no or has little business background. The company does not know the goods or services but still wants to buy or sell them.

- A client who is engaged in trading, brokerage or brokerage services and who is engaged in business that is inconsistent with normal business practice, or who has significant changes in the business.

- Concealment of the end-user, final destination, transhipment or both: delivery dates are uncertain or deliveries are planned outside the destination. The forwarding company is listed as the end-user or destination of the product. The shipping method is unusual for the product or destination. When requesting information, the client is circumventing or does not specify whether the goods are intended for local use, export or re-export.

- The supply chain of goods or services is unreasonable for the particular goods.

- Use of pseudonyms and falsified documents to conceal the involvement of the subject of the sanction.

- Common methods of circumvention used to violate and circumvent a sanction include also the following:

    - Bank accounts belonging to the citizens of a country with a high risk of sanctions or proliferation of weapons of mass destruction, who act on behalf of the subject of sanctions;

    - Use of a joint venture, one of the owners of which is the sanctioned entity;

    - Use of bank accounts of diplomatic staff for the benefit of a subject of sanctions;

    - Cyber attacks against financial institutions and virtual currency service providers are used to raise funds and circumvent sanctions.

Annex 3 – Circumstances that may refer to the financing of weapons of mass destruction

This Annex is based on various risk assessments, typologies, data available to Finantsinspektsioon, statistics and findings from on-site inspections, and specific information. It takes into account the services and products provided by financial institutions and their volume and the geographical position of Estonia.

Some of the characteristics listed in this Annex may occur individually or in together in normal or legitimate transactions; therefore, the provided non-exhaustive list should be considered as assistance in identifying the risks involved.

The following does not require a person having specific obligations to apply due diligence measures in all single cases and request additional information to identify potential risks. A person having specific obligations must make a decision on requesting additional information or a need for that in a risk-based manner.

Sources of funding related to the proliferation of weapons of mass destruction may be legal or illegal. In the event of money laundering, the alert is that the source of the funds is illegal. With regard to the financing of the proliferation of weapons of mass destruction, the risk is greater in cases where the source of funding is legal but it is intended to conceal a specific commodity or end-user. Therefore, the structural differences in funding money laundering and proliferation of weapons of mass destruction should be taken into account in the assessment of risks when evaluating alerts. At the same time, one of the known typologies is the use of virtual currencies to finance weapons of mass destruction.

In order to determine whether it may be the case of financing the proliferation of weapons of mass destruction, specific information may be required in a particular case, including information on the end-user of the goods and information on the specific goods. The financiers of weapons of mass destruction use sophisticated schemes to conceal their activities, such as the use of letters of credit, shadow firms, agents, brokers, etc.

It should be borne in mind that a single alert is not a clear indicator of the potential funding of the proliferation of weapons of mass destruction and when assessing the alerts, these should be combined and analysed in relation to a specific client profile.

Phases of funding the weapons of mass destruction

The first phase (funding phase) – the proliferator raises funds. The funds may come from own resources, foreign donors, criminal activities.

The second phase (concealment of funds) – the proliferator sends the funds to the international financial system. If no sanctions have been imposed on the state, the funds will be transferred directly. In this phase, the proliferators mostly rely on the networks of companies (including shadow firms) and intermediaries to conceal any connection with the sanctioned state. An opaque ownership structure is used to circumvent the sanction. Often, the funding of the proliferation of weapons of mass destruction involves a sanctioned country or its nearby country, and the decisions concerning the company's funds are under the control of a foreign citizen who supports the sanctioned country. Such activities, combined with the use of falsified documents, enable the proliferator to avoid the identification of them and their transaction.

Third phase (procurement of materials and technology) – the proliferator uses the funds to pay for the goods, materials, technology and logistics needed for the programs related to the weapons of mass destruction. Throughout the third stage, international financial institutions are involved in the processing of transactions. It is important to note that proliferation includes not only the purchase of weapons but also individual goods and components that can be used to develop weapons or missiles. Proliferation includes not only the purchase of weapons but also individual goods and components that can be used to develop weapons or missiles. This makes it harder to prevent the proliferation of weapons of mass destruction.

Alerts related to the funding of the proliferation of weapons of mass destruction (the list is non-exhaustive):

- The client is involved in dual-use, supply, sale, delivery or purchase of weapons of mass destruction or military goods, especially in higher-risk jurisdictions.

- The counterparty is located in a country or region with a high risk of funding of weapons of mass destruction.

- The counterparty is located in a country or region where there is a high risk of circumvention of sanctions (goods are diverted to a destination other than the indicated final destination).

- The final destination of the imported/exported goods is unclear in the transaction documents.

- In the case of goods financing transactions, the goods are routed through countries with weak export control laws or where the implementation of export control laws is weak.

- The counterparties are persons or entities located in countries with weak export control laws or low compliance with export control laws.

- The goods involved in the transaction are not customary for the country concerned.

- The route of the goods indicated in the transaction does not correspond to the usual trade pattern and has no commercial logic.

- The transaction involves financial institutions that have been identified as having shortcomings in the prevention of money laundering and terrorist financing, as well as financial institutions domiciled in countries where export control laws are weak or where enforcement of export control laws is weak.

- The transaction documents indicate that the value of the declared goods is undervalued compared to the cost of transport.

- There are inconsistencies in the transaction documents, such as names, companies, addresses, destination, etc.

- Client's activity does not match the company profile or the information on the end-user does not match the end-user company's profile.

- The companies or persons ordering the goods are from countries other than the specified end-user country.

- The information provided by the client, incl., despite the requests for additional information, is vague/incomplete.

- The address of the client or counterparty is similar to the address of the subject of sanctions.

- The transaction has connections between the seller's and buyer's companies, such as the same owners or management.

- The transaction involves potential shadow companies.

- The forwarding company is mentioned as the final destination of the product.

- The originator the payment order or remitter of the payment are not mentioned in the original documents related to the transaction.

- The pattern of client's transactions is unusual or lacks a clear purpose.

- The documents related to the transaction show signs of forgery.

Annex 4 – Differences in the financing of money laundering, terrorist financing and proliferation of weapons of mass destruction[24]

	Money laundering	Terrorist financing	Funding of the proliferation of the weapons of mass destruction
Purpose	Use of illegal means in a regulated system	Support the activity of terrorists	Acquisition of weapons of mass destruction
Origin of funds	From criminal organisations	Own funds, fundraisers, donations	Programs financed by states
Channels	Prefers official financial system	Prefers cash couriers, unofficial financial systems (*hawala*, currency exchange firms)	Prefers official financial system
Focus of identification	Suspicious transactions, for example, transactions that do not correspond to the client's wealth or expected activity	Suspicious relationships, bank transfers between seemingly unrelated parties	Persons, entities, countries, goods and materials, activities
Transaction value	large amounts, often structured, to avoid the notification obligation	Small amounts, usually below the notification threshold	Average amounts
Financial activity	Sophisticated network of transactions, often used by shadow and offshore companies, etc.	Different methods, including the official banking system, unofficial currency transfer systems, cash and valuables smuggling	Transactions look like normal business activities that are structured to conceal the origin of funding

[24] *Jonathan Brewer, Study of Typologies of Financing of WMD Proliferation, Kings College, London, 2017.*