

Finantsinspeksioon

**Advisory Guidelines of Finantsinspeksioon  
“Application of international financial sanctions in credit and financial institutions”**

Established by Resolution No 1.1-7/177 of the Management Board of Finantsinspeksioon of 25.10.2021 and amended by Resolution No 1.1-7/43 of the Management Board of Finantsinspeksioon of 09.03.2026

## CONTENTS

1.	Competence of Finantsinspektsioon.....	3
2.	Purpose, scope of application, underlying principles.....	3
2.1.	Purpose.....	3
2.2.	Scope of application .....	4
2.3.	Underlying principles .....	4
2.4.	Definitions .....	6
3.	Management of international sanction risks .....	7
3.1.	Strategy.....	7
3.2.	Risk assessment and risk appetite .....	8
3.3.	Rules of procedure .....	11
3.4.	Due diligence measures for the identification of financial sanctions.....	12
3.5.	Identification and application of a financial sanction, compliance with the reporting obligation .....	14
3.6.	Data retention .....	15
3.7.	Internal control and internal control rules .....	15
3.8.	Training of employees .....	16
3.9.	Appointment of responsible management board member and responsible person and liability of management .....	16
4.	Implementation of the Guidelines .....	17
	Annex 1 – Automated screening tool .....	18
	Implementation of screening technology rules .....	18
	Ensuring the appropriateness of AST .....	19
	Assessment of warning messages arising from screening technology .....	20
	Measures applied in parallel with screening technology .....	20
	Testing.....	20
	Annex 2 – Assessment of risks related to evasion and breaches of sanctions specific to Estonia .....	23
	Sanction risks and ways to evasion may be related to, inter alia: .....	24
	Warning signs of transactions related to activity-based financial sanctions and evasion methods may be, among other things:.....	24

## 1. Competence of Finantsinspektsioon

- 1.1. Pursuant to § 3 of the Financial Supervision Authority Act (hereinafter the FSAA), financial supervision is conducted by Finantsinspektsioon (Estonian Financial Supervision Authority, hereinafter the FSA) 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 (hereinafter Estonia).
- 1.2. According to § 30 (1)<sup>1</sup> of the International Sanctions Act (hereinafter the ISA), the FSA exercises supervision over compliance with the ISA and the legislation adopted on the basis thereof by credit institutions and financial institutions subject to its supervision under the FSAA and in accordance with the legislation of the European Union. The FSA exercises supervision in accordance with the procedure provided for in the FSAA, taking into consideration the variations provided for in the ISA.
- 1.3. The task of the FSA in the implementation of financial sanctions is to not make exceptions or give permission for the provision of services or for the conclusion of a transaction or an act. The FSA, inter alia, does not check whether a person is a subject of a financial sanction, whether a transaction or act breaches financial sanctions or whether a financial sanction has been lawfully implemented.
- 1.4. The task of the FSA in the implementation of financial sanctions is to exercise supervision over the systems and controls implemented by the Person with specific obligations<sup>1</sup> so that the Person with specific obligations is capable of applying a financial sanction and to assess the risk of a financial sanction (threats, vulnerability, compensation mechanisms).
- 1.5. Pursuant to § 57 (1) of the FSAA, the FSA has the right to issue advisory guidelines to explain legislation regulating the activities of the financial sector and provide guidance to subjects of financial supervision.
- 1.6. These advisory guidelines (hereinafter the *Guidelines*) must be read in conjunction with the advisory guidelines of the FSA “Organisational approaches and preventive measures of credit and financial institutions for the prevention of money laundering and terrorist financing”<sup>2</sup> (hereinafter *the Advisory AML Guidelines of the FSA*), taking into consideration the particularities of international sanctions and prevention of proliferation financing. The Advisory AML Guidelines of the FSA are applied in all issues not regulated in these Guidelines.

## 2. Purpose, scope of application, underlying principles

### 2.1. Purpose

- 2.1.1. The purpose of these Guidelines is to give explanatory instructions for the application of financial sanctions. The activities for the application of financial sanctions have been specifically kept in mind where obligations or sanctions and their implementation in general have been referred to in the Guidelines. Nevertheless, Persons with specific obligations must be aware of the operational and other risks related to their activities and

---

<sup>1</sup> The definition of a Person with specific obligations can be found in clause 2.2.1 of these guidelines.

<sup>2</sup> “Organisational solutions and preventive measures for credit and financial institutions to take against money laundering and terrorist financing” established by Resolution No 1.1-7/172 of 26.11.2018 and amended by Resolution No 1.1-7/58 of 08.04.2024 of the Management Board of the Financial Supervision Authority. Online: [https://www.fi.ee/sites/default/files/2024-06/Finantsinspektsiooni%20rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20juhend\\_0.pdf](https://www.fi.ee/sites/default/files/2024-06/Finantsinspektsiooni%20rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20juhend_0.pdf). (06.10.2025)

assess and handle these in the interests of clients.

- 2.1.2. The purpose of the Guidelines is to contribute to enhancing the capability of Persons with specific obligations that are supervised by the FSA to apply financial sanctions and identify subjects of financial sanctions with the ultimate goal of ensuring that the application of a financial sanction imposed with a resolution of the UN Security Council (hereinafter the UN), a regulation of the Council of the European Union (hereinafter the EU) or a regulation of the Government of the Republic of Estonia (hereinafter the Government of the Republic) or established by other legislation or agreement that imposes obligations on Estonia through the compliance framework of Persons with specific obligations. The Guidelines are only limited to financial sanctions the implementation of which is binding in Estonia.
- 2.1.3. The Guidelines explain the content and fulfilment of the requirements for implementation of financial sanctions established in the ISA and the directly related legislation to Persons with specific obligations, as well as provide an understanding of the risks associated with service provision. These also guide and assist Persons with specific obligations in the development of and ensuring the functioning of the system for sanction risk management in order to apply financial sanctions.
- 2.1.4. The establishment of the Guidelines and their implementation by Persons with specific obligations helps identify subjects of financial sanctions more efficiently and apply financial sanction measures, reduce the probability of the Estonian financial sector being used for criminal purposes and systemic risks, and increase the stability, reliability and transparency of the financial sector.

## **2.2. Scope of application**

- 2.2.1. The Guidelines are aimed at the credit and financial institutions<sup>3</sup> providing services in Estonia that are Persons with specific obligations pursuant to § 20 (1) of the ISA and in respect of compliance with the requirements stipulated in § 21 of the ISA and are subject to supervision by the FSA (hereinafter Persons with Specific Obligations<sup>4</sup>). At the same time, the guidance and recommendations given in the Guidelines should also be taken into account in their risk management by a wider range of subjects, i.e. primarily by persons subject to supervision by the FSA who have obligations under the ISA, in particular in the application of financial sanctions, the effective compliance with which requires actions to ensure the existence of an appropriate system, including risk assessment, the establishment of an organisational solution and the drafting of internal rules. The Guidelines are applied to such subjects as far as the obligations imposed on them by law are concerned, irrespective of the wording of the Guidelines which refer to Persons with Specific Obligations.
- 2.2.2. The FSA may establish annexes to these Guidelines in order to provide Persons with Specific Obligations with sector-based guidelines upon identification of the risks related to the provision of services by them. The FSA may amend or supplement the technical annexes to the Guidelines, except the sector-based guidelines specified in this clause, without the inclusion of market participants or other experts.

## **2.3. Underlying principles**

- 2.3.1. The resolutions adopted by the UN that impose sanctions are implemented in Estonia mainly through EU legislation and, where necessary, the Government of the Republic may issue a legal act for implementing a sanction established by the UN. A sanction

---

<sup>3</sup> In these Guidelines, financial institutions also include providers of crypto asset services pursuant to § 6 (2)(3<sup>1</sup>) of the MLTFPA.

<sup>4</sup> The term used throughout the Guidelines 'The Person with Specific Obligations', is the same as the term 'Person with special obligations' used in the ISA.

established with a resolution of the UN Security Council is temporarily implemented on the basis of the UN Security Council Resolution until a regulation of the Council of the European Union is updated or adopted. The EU can also supplement the sanction of the UN and establish an autonomous EU sanction. A sanction of the Government of the Republic is established by a regulation of the Government of the Republic.

- 2.3.2. UN Security Council resolutions, EU regulations or regulations of the Government of the Republic must be considered upon the application of a financial sanction.
- 2.3.3. In the case of requirements arising from legislation, the provisions of sanction legislation must be adhered to. If the Guidelines are in conflict with legislation, the meaning and content of the ISA and the legislation directly related thereto must be followed. In the case of legislation and source materials directly related to the ISA that are in English<sup>5</sup>, the original wording and meaning must be proceeded from.
- 2.3.4. The terms used in the Guidelines have been defined in the ISA, legislation implementing international sanctions, the glossaries of the 2012 recommendations<sup>6</sup> and 2013 methodology of the Financial Action Task Force<sup>7</sup> (hereinafter the FATF), the guidelines issued by the EU<sup>8</sup>, the guidelines of the Financial Intelligence Unit<sup>9</sup> and other guidance materials, and partially also in clause 2.4 [bookmark34](#) of these Guidelines.
- 2.3.5. Compliance with the requirements for the implementation and application of international sanctions includes, within the meaning of these Guidelines, all of the activities expected from EU, UN and FATF Member States and Persons with Specific Obligations upon the application of preventive measures. In addition, a Person with Specific Obligations must comply with the requirements of the competent authorities of the Republic of Estonia.
- 2.3.6. The requirements arising from effective legislation, international practice and the legislation directly related to the ISA, the other advisory guidelines of the FSA and the guidelines and other guidance materials of the Financial Intelligence Unit, the EBA<sup>10</sup>, FATF and the Council of the European Union must be taken into consideration upon the implementation of these Guidelines.<sup>1112</sup>
- 2.3.7. The principle of proportionality must be followed upon compliance with the Guidelines. This means that a Person with Specific Obligations must prepare their own rules of procedure and internal control rules, apply due diligence measures and choose any means according to the nature, scope and level of complexity of their company's

---

<sup>5</sup> Including legislation implementing international sanctions.

<sup>6</sup> The FATF Recommendations (2012). Online: <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf>. coredownload.inline.pdf. (07.10.2025)

<sup>7</sup> The FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems. Online: <http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf>. (07.10.2025)

<sup>8</sup> Guidelines and Best Practices. Online: <https://www.consilium.europa.eu/en/policies/sanctions/>. (06.10.2025)

<sup>9</sup> Guidelines of the Financial Intelligence Unit for implementation of financial sanctions approved by the Directive of the Head of the Financial Intelligence Unit of 30.05.2025. Online: [https://fiu.ee/sites/default/files/documents/2025-05/Rahapesu%20Andmeb%C3%BCroo%20juhend%20finantssanktsioonide%20kohaldamiseks\\_Kinnitatud%2030.05.2025.pdf](https://fiu.ee/sites/default/files/documents/2025-05/Rahapesu%20Andmeb%C3%BCroo%20juhend%20finantssanktsioonide%20kohaldamiseks_Kinnitatud%2030.05.2025.pdf). (07.10.2025)

<sup>10</sup> EBA Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures (EBA/GL/2024/14) and EBA Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures under Regulation (EU) 2023/1113 (EBA/GL/2024/15), which have been issued as advisory guidelines of the FSA by Resolution 1.1-7/68 of the Management Board of the FSA of 05.05.2025. Online: [https://www.fi.ee/sites/default/files/2025-05/pp%20nr%2007%20EBA%20suunised\\_Gis%20on%20restrictive%20measures.pdf](https://www.fi.ee/sites/default/files/2025-05/pp%20nr%2007%20EBA%20suunised_Gis%20on%20restrictive%20measures.pdf) (09.10.2025) (hereinafter the EBA Restrictive Measures Guidelines)

<sup>11</sup> Incl. the general guidance materials concerning the organisation and activities of financial institutions.

<sup>12</sup> As the relevant documents (e.g. the EBA Guidelines) and the requirements contained therein are constantly changing, the most up-to-date documents and requirements, which may differ from those set out in this version of the Guidelines at any given time, should always be taken into account when applying the Guidelines.

economic activities, including risk appetite and risks associated with the activities of the Person with Specific Obligations.

- 2.3.8. The principle of a risk-based approach must be taken into consideration upon compliance with the Guidelines. Persons with Specific Obligations must assess the risks associated with their activities in advance in order to plan, develop and maintain a system for the reduction of international sanction risk and a risk management system that complies with their capacity, risk appetite and risks associated with their activities, considering that a risk-based approach does not release a Person with Specific Obligations from the imposition of a sanction. Failure to comply with an obligation or breach of a prohibition in legislation implementing an international sanction is a breach of the international sanction.
- 2.3.9. In the case of problems with the application and interpretation of the Guidelines, the principle of reasonableness must be followed, interpreting the clauses of the Guidelines in conjunction with one another and taking into consideration the purpose of these Guidelines. It is also necessary to act in good faith and in compliance with the due diligence expected from a Person with Specific Obligations.
- 2.3.10. A 'comply or explain' principle applies to the Guidelines, which means that the Person with Specific Obligations must be able to justify, where necessary, why they do not implement some clauses of the Guidelines or implement them only partially.
- 2.3.11. It may be necessary to apply measures differing from the Guidelines or additional measures under certain circumstances in order to identify and manage international sanction risks, which is why a Person with Specific Obligations cannot justify non-compliance with legislation simply with the fact that they followed these Guidelines word-for-word.
- 2.3.12. In the case of questions related to the legislation regulating the implementation of an international sanction, the Person with Specific Obligations will not remove themselves in communication with clients. Where necessary, the Person with Specific Obligations must explain to the customer the necessity of the requirements in the public interest.<sup>13</sup> For this purpose, the Person with Specific Obligations creates customer service solutions in such a manner that the requirements arising from legislation and the Guidelines are built into the solutions as well as possible, thereby guaranteeing the smoothest customer service solution possible while complying with the obligations arising from legislation and the recommendations made in the Guidelines.

## 2.4. Definitions

**International sanction**<sup>14</sup> is defined in § 3 (1) of the ISA as an essential tool of foreign policy aimed at supporting the maintenance or restoration of peace, international security, democracy and the rule of law, following human rights and international law or achieving other objectives of the Charter of the United Nations or the Common Foreign and Security Policy of the European Union. Pursuant to subsection (2), an international sanction is imposed on a state, territory, territorial unit, regime, organisation, association, group or person by a resolution of the United Nations Security Council, a decision of the European Council or other law-imposing obligations on Estonia. Pursuant to § 4 (1) of the ISA, the Government of the Republic also has the right, in addition to the aforementioned purposes, to impose a sanction of the Government of the Republic to protect the security or interests of Estonia. International sanction measures may be (1) *non-economic* or (2)

---

<sup>13</sup> When providing explanations to a client, it must be taken into account that, inter alia, this does not jeopardise the confidentiality of the proceedings, does not reveal the logic of the risk assessment models of the Person with Specific Obligations and is in accordance with the restrictions set out in § 51 of the MLTFPA.

<sup>14</sup> The term 'restrictive measure' is used in EU legislation, guidance materials and other documents, including EBA guidelines. In accordance with the terminology used in Estonian legislation, the term 'sanction' is used in these Guidelines.

*economic*. Economic measures may, in turn, be divided into (a) *international financial sanctions* and (b) *commercial sanctions*.

**The subject of an international sanction** means a natural person or legal person, entity or agency specified by a general characteristic or list in legislation imposing or implementing an international sanction to whom an international sanction is applied. Thus, the subject of an international sanction may also mean a state, a territory, a territorial unit, a regime, an organisation, an association, a group or another unit to whom a sanction is applied and who has been specified as a subject in legislation imposing or implementing an international sanction.

**An international financial sanction** (a sub-type of economic sanction) is primarily a targeted measure aimed at specific persons or countries/regions. Financial sanctions are thereby largely divided into sanctions for terrorist financing and proliferation financing and sanctions of other political content and purpose. The content of a financial sanction is to prohibit or limit any transfer, change, use of funds or conclusion of transactions with them that could bring about changes in their volume, size, location, ownership, possession, nature or purpose or other changes that would allow for the use of such funds. The content of a financial sanction is also to prohibit the use of economic resources (assets which are not financial resources but can be used for the acquisition of financial resources, goods or services) in any manner for the acquisition of financial resources, goods or services, e.g. by selling or renting them or establishing a mortgage on them. A financial sanction can be divided into (i) *targeted* and (ii) *activity-based*. The exact measures of international financial sanctions that must be applied and the persons to whom they must be applied are described in the legislation imposing or implementing international sanctions.

**A targeted financial sanction**<sup>15</sup> is imposed on an individual or entity and refers to (a) the freezing of funds and economic resources, (b) not making funds and economic resources available or (c) prohibiting the use of the financial system to a person or entity added to the international sanctions list.

**An activity-based financial sanction** restricts or prohibits certain activities. For example, funding, financing (including investing), entering into an insurance contract, concluding securities transactions, lending and entering into or continuing a business relationship related to these activities, providing advice or other financial services. The subject of an activity-based financial sanction is not necessarily identified by name. The restriction or prohibition is usually targeted at a specific group of persons, a sector or a region, based on some characteristic.

**Proliferation financing** means an act for the provision of financial resources or the provision of financial services that are fully or partially used for the production, acquisition, possession, development, export, reloading, mediation, transport, transfer, procurement or use of nuclear, chemical or biological weapons, their carriers and the materials associated with them (including technology as well as goods of dual use used for unlawful purposes), which is in conflict with national laws or, if necessary, international obligations.<sup>16</sup> Financial sanctions, both targeted and action-based, are one of the main tools to prevent proliferation financing and the illicit trafficking of strategic goods.

### 3. Management of international sanction risks [bookmark46](#)<sup>17</sup>

---

<sup>15</sup> Targeted Financial Sanctions or TFS.

<sup>16</sup> The definition of proliferation financing is based on the FATF report "Combating proliferation financing: A status report on policy development and consultation" (2010). Online: <https://www.fatf-gafi.org/media/fatf/documents/reports/Status-report-proliferation-financing.pdf>. (11.10.2025)

<sup>17</sup> The term 'risk mitigation and risk management system' is used in the ISA, but as risk mitigation is part of risk management, the term risk management is used throughout the Guidelines.

### **3.1. Strategy**

- 3.1.1. The overall strategy for managing international sanction risks describes the general guiding principles observed by Persons with Specific Obligations to ensure that their activities are in accordance with their risk appetite. The overall strategy for managing international sanction risks may be included in the risk appetite of Persons with Specific Obligations.
- 3.1.2. The international sanction risk management strategy is reviewed, updated and supplemented, if necessary, including when the risk position of the Person with Specific Obligations changes, the risk assessment or risk appetite is updated and supplemented or if new sanction regimes are added.

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

- 3.2.1. A Person with Specific Obligations regularly prepares and updates their risk appetite and risk assessment related to financial sanctions and proliferation financing, taking into consideration the principles set out in clauses 3.2 and 3.3 of the Advisory AML Guidelines of the FSA with the exceptions set out in the Guidelines and characteristic of the area of proliferation financing.
- 3.2.2. The financial sanctions and proliferation financing not only covers direct breaches of financial sanctions, e.g. not freezing the financial assets of the subject of sanctions, but also evasions of financial sanctions. Persons with Specific Obligations must observe this principle upon the identification, assessment and analysis of risks.
- 3.2.3. The risk factors characteristic of a financial sanction must be analysed within the meaning of clause 3.2.5.1 of the Advisory AML Guidelines of the FSA in the case of specific risk categories within the scope of financial sanction risk assessment:
- 3.2.3.1. Risks related to clients – client risk refers to possible client categories whose activities involve a higher financial sanction and proliferation risk. One of the most common characteristics is the complexity of the ownership and/or management structure, i.e. how easy or difficult the identification of managers and beneficiaries, including owners, is. In the case of ownership structure, the risks related to the companies managed or owned by the client are also significant (e.g. if the client is the beneficiary of a company that is the subject of sanctions). This means that a Person with Specific Obligations should apply enhanced due diligence measures to assess the clients whose ownership structure is complicated or entails another risk. In the case of risks related to clients, risks related to the business activities of clients, i.e. the area of activity and products and services offered, as well as the geographic risks, such as the customer's origin, usual place of stay, registration location and place of business, must also be taken into consideration.
- 3.2.3.2. Risks related to products, services and transactions – the product, service or transaction risk is related to the products and services provided by a Person with Specific Obligations which carry a high sanction risk or which the client may take advantage of in order to evade sanctions. For example, the volume of cross-border transactions carried out by the Person with Specific Obligations, the number of cross-border correspondent bank accounts and the countries in which they are held; does it provide products related to trade financing; payable-through accounts; crypto asset exchange, safekeeping, transmission and other services; correspondent bank services, etc. Web-based products and services may pose a higher risk due to the speed of processing payments and the anonymity of access to accounts, which is why this risk category is also exposed to risks related to service transmission channels.
- 3.2.3.3. Supply channel<sup>18</sup> risks – the supply channel risk is related to the service and product

---

<sup>18</sup> Transmission, sales, marketing, communication and intermediation channels may also be regarded as supply

transmission channels used by the client upon the establishment of business relationships and during business relationships as well as the channels used by Persons with Specific Obligations in their business activities for selling their products and services. In terms of financial sanction risk, the aforementioned primarily covers the risk of products and services that can be consumed anonymously, which is why a Person with Specific Obligations is unable to identify the location of the customer of the service (e.g. IP addresses are masked or the service is used through intermediaries or representatives, including lawyers/attorneys). It is also risky if the client uses a broker or agent to deal with a Person with Specific Obligations. It is also important to assess the risks associated with supply channels if the due diligence measures applied by a third-party service provider are relied on or if the due diligence obligation has been outsourced, especially if such a service provider is located in a jurisdiction where lower compliance standards are applied according to international assessments. Other service provision channels, such as the online bank and its accessibility, must also be assessed.

- 3.2.3.4. Geographic risks – Geographic risk is related to the exposure of the client, the products and services provided and the supply channels of Persons with Specific Obligations to higher-risk jurisdictions. The risks related to the country of location of the Person with Specific Obligations and the risks arising from the geographic, cultural and historical links of this country of location and the country subject to sanctions must be taken into consideration in the case of this risk category. Situations where transactions are directly or indirectly related to a country or region of a sanction risk must also be taken into consideration. In addition to countries and regions on which sanctions have been imposed, countries and regions through which sanctions may be evaded must also be taken into account. In the context of geographic risk, it is important to understand any indirect risks that may additionally arise if the transaction is related to a high sanction risk (e.g. the product supply chain). As a result of the assessment of geographic risks, Persons with Specific Obligations should determine which sanctions lists should be screened for all jurisdictions and whether and which lists should be screened in respect of certain jurisdiction(s).
- 3.2.3.5. The risks related to the systems used to identify the subject of a financial sanction, including technology – it is important to note that even small parts of a system have a significant impact on the system as a whole, so any decision affecting the effectiveness of the system should be based on a prior risk analysis (be risk-based). If a Person with Specific Obligations uses an automated screening tool (hereinafter AST) for financial sanctions when applying due diligence measures, they shall assess, inter alia, risks related to the capability of the technology and manipulation, including the potential (risks) of proliferation financing and evasion. Before the introduction of new technology, including both in-house and outsourced technology, it is necessary to learn about the technology and to analyse and assess the risks related to its introduction, and the organisation must have the capacity to use the technology in the best possible way, i.e. competent staff and consistent AST control and validation. Thus, the risks associated with systems, including technology, are very institution-based and relate to all the risk categories listed above. In order to manage these risks, it is necessary to ensure that the system is analysed before introduction and that all aspects of the system are consistently controlled.
- 3.2.4. The sanction risks, including the risks of proliferation financing, to which the Person with Specific Obligations is exposed are determined on the basis of a methodology similar to the methodology used to analyse the risk of money laundering and terrorist financing by assessing the following:
- Inherent risk of a Person with Specific Obligations – the sanction risk to which the organisation is exposed without sanction risk management and mitigation measures
  - Efficiency of the sanction risk management and mitigation measures

---

channels.

- Scale of residual risk (by assessing the inherent risk and the efficiency of mitigation measures)
- 3.2.5. The following formula is used to determine the sanction risk identifier characteristic of a Person with Specific Obligations:  
inherent risk – efficiency of sanction risk management and mitigation measures = residual risk
- 3.2.6. A Person with Specific Obligations must separately assess the risks of money laundering, terrorist financing and financial sanctions by preparing a risk assessment for this purpose. Risk assessments may be in a single document, but different risks must be separately assessed. As part of the financial sanction risk assessment, a Person with Specific Obligations must have separately identified and understood, among other things, the proliferation financing risk characteristic of its business, which arises from a possible breach, non-application or evasion of financial sanction requirements. The evasion risks must therefore be assessed separately, appropriate measures must be created to manage this risk, and compliance with and monitoring of them must be ensured.
- 3.2.7. A Person with Specific Obligations determines the risk appetite on the basis of a risk assessment. The provisions of clause 3.3 of the Advisory AML Guidelines of the FSA are applied to risk appetite. The risk appetite of a Person with Specific Obligations can also be described in the risk management strategy for international sanctions. In the case of risk appetite, the Person with Specific Obligations considers that the choice and application of measures is risk-based, but in the case of a situation requiring the application of a sanction, including suspicion, they must act on the basis of rules, i.e. the sanction must be applied in any case.
- 3.2.8. As a result of the risk assessment and risk appetite, the Person with Specific Obligations establishes an international sanction risk management system<sup>19</sup>, for the management of sanction risks, documents and updates the system and its components, and takes them into account in the performance of the tasks set forth in the ISA. Similarly to risk assessment, the possibility of evasion of the financial sanction and the management of this risk must also be taken into consideration in addition to the risk of a breach of a financial sanction when the risk management system is established.
- 3.2.9. The international sanction risk management system must be described in writing and include, inter alia:
- 3.2.9.1. the risk mitigation and risk management strategy (clause 3.1 of the Guidelines);
  - 3.2.9.2. the establishment and updating of risk appetite and risk assessment (clauses 3.2 and 3.2.6 of the Guidelines);
  - 3.2.9.3. the establishment and updating of the guidelines and rules of procedure describing the management and mitigation of risks (clause 3.3 of the Guidelines);
  - 3.2.9.4. the control measures to be taken to manage the risks, including the procedures and extent of due diligence measures to be applied (clause 3.4 of the Guidelines);
  - 3.2.9.5. the identification and application of a financial sanction, compliance with the reporting obligation (clause 3.5 of the Guidelines);
  - 3.2.9.6. the collection and retention of data (clause 3.6 of the Guidelines);
  - 3.2.9.7. the performance of internal control (clause 3.7 of the Guidelines); and

---

<sup>19</sup> In the context of these Guidelines, the risk management system covers all three lines of defence.

- 3.2.9.8. an appropriate training programme (clause 3.8 of the Guidelines).
- 3.2.9.9. In addition to the above, it is important to appoint responsible persons and define their responsibilities (clause 3.9 of the Guidelines).
- 3.2.10. The principles and rules of how a Person with Specific Obligations shall identify high-risk transactions, products, services, clients and geographic regions are defined in the international sanction risk management system. The risk mitigation and risk management system is proportional and takes into consideration the practical needs and the nature, scope and complexity of the economic or professional activities of the Person with Specific Obligations.
- 3.2.11. The international sanction risk management system must be clear and easily understandable, give a clear overview of the entire organisation and define the roles and responsibilities. The system includes standards and requirements that must be complied with and the compliance with which is consistently monitored.
- 3.2.12. The international risk management system includes rules of procedure and internal control rules that provide the guidelines for identification of subjects of financial sanctions, the application of financial sanctions, including safekeeping of frozen funds, reporting and the control measures used to mitigate or manage the risks arising from the financial sanction. Among other things, the international risk management system provides an overview of and guidelines on how to behave in a situation where a subject of financial sanctions, a higher risk or a sign of a threat is identified. This includes a description of the activities of the Person with Specific Obligations before a decision on the application of financial sanctions, refusal to conclude a transaction or refusal to provide services is made.

### **3.3. Rules of procedure**

- 3.3.1. The rules of procedure and guidelines for international financial sanctions describe the principles and action plans for the application and identification of financial sanctions. The rules of procedure define the operating principles for checking, inter alia, the client base, the transactions concluded by Persons with Specific Obligations and the identification of situations that require the application of financial sanctions.
- 3.3.2. The rules of procedure correspond to the practical needs of the Person with Specific Obligations and the nature, scope and level of complexity of their economic or professional activities, including the risk appetite and risks arising from the activities of the Person with Specific Obligations, and are in written format or in a format that can be reproduced in writing.
- 3.3.3. The Person with Specific Obligations establishes rules of procedure, which are used to efficiently manage the risks related to the financial sanctions and proliferation financing and which guarantee an organisational structure that makes it possible to promptly detect the entry into force, amendment or expiry of a financial sanction. The rules of procedure of a Person with Specific Obligations must include at least the following guidelines:
  - 3.3.3.1. how to identify a subject of international financial sanctions and a transaction or act that breaches financial sanctions
  - 3.3.3.2. how to act in the event of suspicions concerning the identification of a subject of international financial sanctions or a transaction or act that breaches financial sanctions
  - 3.3.3.3. the procedure for identification of the risk of a breach of an international financial sanction and how to act when such a risk is identified, including the procedure for identification and investigation of possible breaches or evasion of financial sanctions, including the procedure for the timely identification of a financial sanction and the risk of proliferation

financing before the transaction, an occasional transaction or the establishment of a client relationship and during the entire business relationship and guidelines for freezing assets, restricting access to services and the implementation of other relevant sanction measures;

- 3.3.3.4. the implementation of due diligence measures, including collection of additional data, e.g. when to request additional information from a partner or client and how to retain the data collected (see also clause 3.4 of the Guidelines);
- 3.3.3.5. on compliance with the reporting obligation (see also clause 3.5 of the Guidelines);
- 3.3.3.6. on the retention of data and making them accessible (see also clause 3.6 of the Guidelines).
- 3.3.4. A Person with Specific Obligations appoints the responsible persons and their tasks and competencies with the rules of procedure.
- 3.3.5. The rules of procedure regulate the movement of information concerning financial sanctions and proliferation financing in the company.
- 3.3.6. A Person with Specific Obligations introduces the rules of procedure, guidelines, etc. to all of their employees whose duties include the establishment and monitoring of business relationships or the conclusion of transactions and internal control operations.
- 3.3.7. The rules of procedure and guidelines are reviewed regularly and updated, if necessary.

#### **3.4. Due diligence measures for the identification of financial sanctions**

- 3.4.1. A Person with Specific Obligations creates a process for checking subjects of financial sanctions and for determining sanction risk levels in respect to existing clients as well as upon the establishment of new client relationships. This solution is based on sanctions lists, the obligations and restrictions arising from sanction regimes, the data collected upon the application of the due diligence measures arising from the Money Laundering and Terrorist Financing Prevention Act (hereinafter the MLTFPA) and financial sanction-specific due diligence measures, such as screening, and the data collected during an investigation carried out independently by the Person with Specific Obligations.
- 3.4.2. The Person with Specific Obligations ensures the use and updating of a client's data during the business relationship, including upon verification of the client's transactions to rule out breaches of the financial sanction and prevent evasion of the financial sanction.
- 3.4.3. The Person with Specific Obligations implements the financial sanction due diligence measures:
  - 3.4.3.1. upon the establishment of a business relationship;
  - 3.4.3.2. during the business relationship;
  - 3.4.3.3. upon the conclusion of transactions, including occasional transactions;
  - 3.4.3.4. upon the risk or suspicion of a breach of the financial sanction.
- 3.4.4. When applying the financial sanction due diligence measure specified in clause 3.4.3 of the Guidelines, the Person with Specific Obligations considers the due diligence measures set out in the MLTFPA, taking into account the specific nature/specificities of the financial sanction risks, including monitors the business relationship. Upon the application of due diligence measures, the Person with Specific Obligations collects additional information, including on:

- 3.4.4.1. whether a person that is in or plans to enter into a business relationship with it is the subject of a financial sanction;
- 3.4.4.2. whether the transaction or operation planned or to be concluded breaches a financial sanction;
- 3.4.4.3. the purpose and nature of the business relationship, transaction or operation.
- 3.4.5. The Person with Specific Obligations verifies the additional information received on the basis of documents, data or information obtained from a credible and independent source.
- 3.4.6. When deciding on the scope of application of sanction due diligence measures, it is important to assess all the aspects related to risks, including the client risk, the risk of the products and services provided by the Person with Specific Obligations, the risk of the sales channel and the geographic risks, and how these risks are managed. It is important to understand the client's geographic market share, including the seat and the place where the client is registered or the client's place of residence, origin and connections, when geographic risk is assessed. The due diligence measures applied by the Person with Specific Obligations are proportional and take into consideration the sanction risks arising from their business activities.
- 3.4.7. The data collected during the application of due diligence measures must be relevant and up to date, taking into consideration the fact that the financial sanctions change over time. The constant updating of due diligence measures is necessary to ensure that the client and transactions are screened (before the conclusion of the transaction) to prevent the breach of a financial sanction or evasion of sanction.
- 3.4.8. The Person with Specific Obligations determines the manner and means of checking whether the client or a person or entity related to them is the subject of a financial sanction and that the conclusion of transactions does not constitute the breach of a financial sanction, including evasion of sanction. These tools may be manual systems as well as the AST.
- 3.4.9. If the Person with Specific Obligations decides to use the AST in its screening system, Annex 1 "Automatic tool for screening" to the Guidelines will apply to them and the principles of a proportional approach set out in Annex 1 will also be taken into consideration.
- 3.4.10. The tools used must be risk-based and proportional, i.e. they must correspond to the size of the Person with Specific Obligations and the nature, scope and level of complexity of their activities and the offered products and services, including the risk appetite and the risks associated with the activities of the Person with Specific Obligations. This means that the bigger the client base of the Person with Specific Obligations (if the Person with Specific Obligations cannot monitor clients and transactions manually) and/or the more transactions the Person with Specific Obligations concludes, especially high-risk transactions, and the bigger the associated risk of a financial sanction, the more tools the Person with Specific Obligations must use for the identification of a situation or risk of a financial sanction and the bigger the scope of such tools must be. Tools with a bigger scope mean automated and technological monitoring and screening programmes, their scope, options, efficiency, etc. The Person with Specific Obligations performs screening manually if the risk is low or there are few transactions and clients [bookmark69](#)<sup>20</sup> or if comparable data cannot be found from reliable sources in digital format or in another format required for automatic screening (e.g. commercial documents).
- 3.4.11. The Person with Specific Obligations carries out media monitoring and uses the

---

<sup>20</sup> Considering clients, the volume and complexity of transactions and the resources in use.

information collected internally during the application of due diligence and the screening of transactions and, if necessary, adds to the internal screening list persons and entities in respect of whom a high risk related to sanctions or proliferation financing has been identified (if any).

- 3.4.12. A Person with Specific Obligations must know their client. A complex (ownership) structure creates additional links between the persons who control the company's activities and the Person with Specific Obligations. This creates a lack of transparency and prevents the Person with Specific Obligations from understanding the substance, purpose and identity of the persons involved in the transaction, including whether it is the subject of a financial sanction or a person under its control, or whether the transaction breaches a financial sanction. The complexity of the (ownership) structure of the company is assessed by applying due diligence measures based on pre-defined rules of procedure of the obliged person. The assessment, together with the relevant criteria, must be documented.
- 3.4.13. The Person with Specific Obligations defines internal control rules and ensures that the lists of sanction subjects used by them are accurate, reliable, up to date, constantly updated and proportionate to the risks managed by the Person with Specific Obligations. In doing so, the Person with Specific Obligations takes into account all relevant sanction regimes applicable in the Republic of Estonia, including sanctions imposed by the Government of the Republic. In addition, internal controls must include controls to ensure that systems, including procedures, are in place to identify the risks of evasion of sanctions, including measures to prevent proliferation financing.

### **3.5. Identification and application of a financial sanction, compliance with the reporting obligation**[bookmark70](#)<sup>21</sup>

- 3.5.1. The Person with Specific Obligations applies a financial sanction according to the legislation that implements the sanction. For this purpose, the Person with Specific Obligations ensures the timeliness and relevance of the systems used to ensure the identification of a sanction, including the lists used.
- 3.5.2. The existence and effective use of lists is part of the compliance framework of the Person with Specific Obligations.
- 3.5.2.1. The updating of lists and the frequency of screening can be risk-based or rule-based.
- 3.5.2.2. The Person with Specific Obligations may screen the client database on a daily basis or when the sanction lists are updated.
- 3.5.2.3. If exceptions are made in transaction screening, these risks must be managed otherwise and the Person with Specific Obligations must be prepared to justify such decisions to the competent supervisory authority.
- 3.5.2.4. All exceptions must be assessed and justified. The Person with Specific Obligations also takes into account that the use of the assistance of any service provider in identifying a situation that requires the application of a sanction does not release the Person with Specific Obligations of the obligation to apply the sanction promptly and lawfully.
- 3.5.3. The identification of a situation requiring the application of a financial sanction and the performance of the reporting obligation must be based on the requirements of the law and

---

<sup>21</sup> As the identification and application of financial sanctions and the performance of the reporting obligation are adequately described in the law and are complemented by the existing guidance materials of the Financial Intelligence Unit, this topic will not be covered in detail in these guidelines. The FSA has the competency to monitor compliance with these obligations.

the guidance materials of the Financial Intelligence Unit<sup>22</sup>. The Person with Specific Obligations ensures that the reports they submit to the Financial Intelligence Unit are of high quality and comply with the requirements of the guidance materials specified above. Submission of low quality reports indicates weaknesses in the system of the Person with Specific Obligations, including in the establishment and use of their own systems, the training of staff and the functioning of compliance.

### **3.6. Data retention**

- 3.6.1. The Person with Specific Obligations collects and retains, inter alia, data related to (i) checks of whether the person who is or plans to be in a business relationship with the Person with Specific Obligations is the subject of a financial sanction; (ii) checks of whether the planned or concluded transaction or operation breaches a financial sanction or creates the risk of evasion; (iii) the application of a financial sanction; and (iv) reporting to the Financial Intelligence Unit. The data collected in the application of due diligence measures (including data on determining the risk level of a client) or on the suspicion or threat of a breach of an international sanction relating to goods or services must also be retained. The obligation to retain the data applies even if the transaction is not concluded as of the date of receipt of the data.
- 3.6.2. The data are retained in a manner that makes it possible to respond to queries of supervisory authorities or other persons entitled thereto exhaustively and immediately.
- 3.6.3. The data arising from clause 3.6.1 (excluding clause (iv)) of these Guidelines must be retained for five years after the expiry of the business relationship or the conclusion of an occasional transaction. The data related to the performance of the reporting obligation arising from clause (iv) must be retained for five years after the performance of the reporting obligation.
- 3.6.4. If the Person with Specific Obligations makes, for the application of due diligence measures, a query to the state's electronic database, the obligations of data retention will be deemed to have been performed if the information about making the electronic query to said register can be reproduced over a period of five years after the expiry of the business relationship or the conclusion of the occasional transaction.

### **3.7. Internal control and internal control rules**

- 3.7.1. The internal control rules are part of the internal control system, which must be sufficiently independent of the controlled business activity. In addition, the internal control carried out by the second line of defence and the internal audit carried out by the third line of defence must be independent of each other. Drafting and applying the internal control rules must be based on the requirements of the MLTFPA and the Advisory AML Guidelines, taking into account the specificities of the area of financial sanctions. The internal control rules are an organisation's internal procedure for checking compliance with the rules of procedure and other similar rules, including for testing the AST if the Person with Specific Obligations uses them. The internal control rules set out, inter alia, the frequency of internal control, the procedure for carrying out internal control and the procedure for retention of results.
- 3.7.2. The internal control rules must include inspection of staff and the tools, including technological solutions such as AST, used by the Person with Specific Obligations. This ensures, inter alia, that the control system for following a financial sanction functions as required and within the prescribed parameters.

---

<sup>22</sup> Including on reporting requirements. See e.g. "Detailed guidance for reporting to the Financial Intelligence Unit" of the Financial Intelligence Unit. Online: [https://fiu.ee/sites/default/files/documents/2024-07/T%C3%A4psustav%20juhis%20teate%20esitamiseks%20Rahapesu%20Andmeh%C3%BCroole\\_23.07.2024.pdf](https://fiu.ee/sites/default/files/documents/2024-07/T%C3%A4psustav%20juhis%20teate%20esitamiseks%20Rahapesu%20Andmeh%C3%BCroole_23.07.2024.pdf). (23.10.2025)

- 3.7.3. The internal control rules must describe the functioning of internal control, including the procedure for the application of internal audits and compliance. Among other things, it must be stipulated who inspects the compliance of the employees, systems, rules of procedure, etc. of the Person with Specific Obligations as well as how and how often this is done. The rules of procedure regulating the performance of internal control must be detailed enough to ensure that the employee gains an understanding of who controls their line of work. In this respect, it is important to distinguish between the regular internal control carried out by the second line of defence and the internal audit carried out by the third line of defence.
- 3.7.4. All inspections and processes related to financial sanctions must be documented. The Person with Specific Obligations prepares inspection and supervision documents, including the procedures for handling suspicious cases. It must be ensured that the documents are up to date and relevant.
- 3.7.5. It is also good practice to present the results of the control to the employee and, if deficiencies are identified, to make suggestions to the management board to introduce necessary changes in the risk identification and management system, the application of due diligence measures or other activities related to compliance with the requirements of the IAS.

### **3.8. Training of employees**

- 3.8.1. Training is part of the international sanction risk management system. The objective of the training is to create and raise awareness among staff of their obligations in the application of an international sanction. Training and knowledge of various international sanctions, typologies, ways of evasion and obligations are necessary so that the employees can apply the necessary due diligence measures and know what action should be taken if they detect a possible breach of an international sanction. Training will help manage and mitigate the international sanction risks that a Person with Specific Obligations may be exposed to. Training must correspond to the specificities of the organisation, i.e. take into account the products and services provided, the clients, partners and geographic region in which it operates and comply with the principle of proportionality.
- 3.8.2. The Person with Specific Obligations ensures that their employees whose duties include the establishment of business relationships or the conclusion of transactions are trained to perform the obligations arising from the ISA and the legislation implementing international sanctions.
- 3.8.3. The training must be tailored to the employees and the specific role, and must take place when the employee's employment commences before the performance of the tasks requiring the training, and regularly or as required during the employment relationship. This training is mandatory, especially for the staff described in clause 3.8.2 of the guidelines and for others according to their role in managing international sanction risks (based on the risk-based approach). The training includes, as a minimum, information on the organisation's international sanction risk assessment and its results, the obligations laid down in legislation and rules of procedure, up-to-date typologies of international sanction breaches and evasion methods and the associated risks, as well as personal data protection requirements. The risks associated with proliferation financing must also be specifically addressed in the training. The Person with Specific Obligations is ready to prove the adequacy and effectiveness of its training courses. This requires documentation of the training plan, among other things. Effectiveness is proven, inter alia, by checklists filled in after training, which show whether the employee has understood and retained the key aspects relevant to their job. Another measure is, for example, internal control, which includes, among other things, the monitoring of the activities of the employees for which they have received training. This also helps understand further training needs.

3.8.4. The provisions of clause 3.9 of the AML Guidelines of the FSA apply to staff training, taking into account the specificities of the financial sanction.

### **3.9. Appointment of responsible management board member and responsible person and liability of management**

3.9.1. Within the meaning of the Guidelines, the provisions of § 17 of the MLTFPA and clause 3.4 of the AML Guidelines of the FSA apply to the liability of the management board and the appointment of the responsible member of the management board.

3.9.2. A Person with Specific Obligations appoints a person responsible for the performance of the duties provided for in the ISA and the Guidelines, including for the implementation of a financial sanction (hereinafter the Responsible Person) and forwards their contact details to the Financial Intelligence Unit and the FSA. A Person with Specific Obligations informs the Financial Intelligence Unit and the FSA in writing within 30 days of the appointment of the Responsible Person or the employee covering for them and their details.

3.9.3. § 17 of the MLTFPA and clause 3.5.3 of the Advisory AML Guideline of the FSA are applied upon the appointment of the Responsible Person of the Person with Specific Obligations and in respect of their duties and rights, taking into account the differences characteristic to the implementation and application of sanctions.

3.9.4. The Person with Specific Obligations ensures that the Responsible Person has adequate skills and knowledge for the performance of the duties related to the application of financial sanctions and for making decisions on lawful action.

3.9.5. The Person with Specific Obligations ensures that the person responsible for the application of a financial sanction has sufficient authorisation and access to the information required for the performance of their duties.

## **4. Implementation of the Guidelines**

The Guidelines are effective as of 11.03.2026. As these Guidelines clarify the applicable law, these do not change the validity of the requirements arising from the legislation. The various explanations in the Guidelines are immediately effective if they are relevant and recognised professional standards in the financial sector, which the Person with Specific Obligations can be expected to be aware of and apply.

## Annex 1 – Automated screening tool [bookmark100](#)<sup>23</sup>

In the case of larger and more complex financial institutions, it is presumed<sup>24</sup> that technology is used as a certain basic function in the screening system in order to ensure the creation and management of relevant warning messages. Such functions include the ability to implement risk-based screening rules. This Annex describes the internationally recognised principles and expectations for the AST, which is integrated into the screening programme. This Annex may not be exhaustive, as technological development is fast and the expectations of Persons with Specific Obligations for the AST may have changed. However, if a Person with Specific Obligations decides to use the AST, they should consider the principle of proportionality set out in clause 3.4.10 of the Guidelines. AST can be both outsourced and developed in-house. In the first case, the requirements to outsourcing in the FSA’s advisory guidelines “Requirements for outsourcing by persons subject to financial supervision”<sup>25</sup> and in the EBA Guidelines on Restrictive Measures must be followed among other things. The establishment of one’s own system requires the organisation to have the respective capacity and the continuous development, inspection and validation of the system. In both cases, the system must allow for the correct and timely application of the sanction, and the Person with Specific Obligations must be able to configure the system of their choice in the best way to meet their obligations (or provide guidance to the service provider on how to configure the system best suited to its risks) and use it.

### Implementation of screening technology rules

The principles of exact matches and fuzzy logic<sup>26</sup> are used in the implementation of ATS rules and it is advisable to combine them. A risk-based approach may be used when setting up the rules for fuzzy logic, taking into account the recommendations in clauses 3.5.2.3 and 3.5.2.4 of the Guidelines. The screening technology may also use additional and restrictive rules, including a whitelist<sup>27</sup> for the data of persons and entities that have previously been identified as incorrect matches and that are not subject to a financial sanction or a client or transaction that entails a high sanction risk. The reasons of the decision on inclusion in the white list must be documented. The use of such lists helps reduce the number of incorrect matches. The whitelist is assessed and updated periodically and immediately when a sanction regime enters into force or changes, when the data of a client change, or when risk factors appear in respect of any person or entity added to the list. It is important to ensure that all sanction regimes applied in the Republic of Estonia are covered, including the list of subjects covered by the sanctions of the Government of the Republic.

According to the risks arising from the activities of the Person with Specific Obligations and its risk appetite, the Person with Specific Obligations determines the appropriate screening threshold(s)<sup>28</sup> for the creation of matches in the AST, which would make it possible to create the appropriate alerts. In order to define a correct, effective and fair screening threshold, the Person with Specific Obligations must be familiar with the AST it uses and the risks of financial sanctions and proliferation financing that are specific to the Person with Specific Obligations. The quality of the data and the control the Person with Specific Obligations has over the screened data are also

<sup>23</sup> These Guidelines are intended to complement the EBA Guidelines on Restrictive Measures and therefore do not repeat all of their contents, but are intended to be used in conjunction with them.

<sup>24</sup> For CASPs and PSPs, the use of a technological solution for screening is required. In addition to this Guide, CASPs and PSPs must also follow the guidance and recommendations in the EBA Guidelines on Restrictive Measures.

<sup>25</sup> The FSA’s advisory guidelines “Requirements for outsourcing by persons subject to financial supervision (new version)”. Online: [https://www.fi.ee/sites/default/files/2024-03/FI%20soovituslik%20juhend%20N%C3%B5uded%20finantsj%C3%A4revalve%20subjekti%20poolt%20tegevuse%20edasiandmisele\\_MUUDETUD.pdf](https://www.fi.ee/sites/default/files/2024-03/FI%20soovituslik%20juhend%20N%C3%B5uded%20finantsj%C3%A4revalve%20subjekti%20poolt%20tegevuse%20edasiandmisele_MUUDETUD.pdf) (28.10.2025) (hereinafter the FSA Outsourcing Guidelines).

<sup>26</sup> The use of the fuzzy logic has many benefits, as it takes partial truth values into consideration. This helps assess the appropriateness of the possible match and define certain conditions for specific matches. By combining both ‘exact match’ and ‘non-exact match’ rules, fuzzy logic can lead to more exact identification, even if the data have been written incorrectly or are incomplete or missing. However, the use of fuzzy logic may not be sufficient if the data are in a specific native language and characters are used and if the data are stored in several systems. The size of the threshold also plays an important role when fuzzy logic is used.

<sup>27</sup> Whitelisting or good guy in English. So-called whitelist.

<sup>28</sup> The screening threshold indicates the correspondence of percentage to a specific name in the list.

considered when the screening threshold is determined. If the Person with Specific Obligations is aware of deficiencies in the quality of their own data or the data of the financial organisation related to the transaction counterparty, the screening threshold must be reduced accordingly. Upon calibration, it must be taken into account that it should not be too sensitive, which would result in AST generating excessively false positive matches, or too insensitive, which would lead to a situation that requires the application of a sanction being ignored. It is important to strike a balance between efficiency and effectiveness. A good screening system catches sanctioned names/matches, but does not generate a large number of alerts per hit.

When applying the screening rules in the AST, the Person with Specific Obligations must keep in mind that some data are in different formats and presented in different ways. Transactions containing such data may require manually performed review processes where the relevant information is manually checked. Good screening quality in the AST is ensured by the high-quality client and transaction data, which are clean or cleaned, used for screening. High-quality data ensure easier and more effective control against sanctions lists. When using the AST, the Person with Specific Obligations establishes transliteration and transcription rules to ensure that the names of people and places can be unambiguously identified and that the spelling is comparable with the indicators on the sanctions list.

The algorithms and screening threshold used in the AST must be reviewed and updated immediately when new patterns, typologies, high-risk factors and false negative matches<sup>29</sup> are identified or when sanction regimes change and new ones are added.

### **Ensuring the appropriateness of AST**

The Person with Specific Obligations ensures that the updates and changes to the sanctions lists (adding to and removing from lists, changing the relevant data of the subjects of sanctions) in the AST are updated and introduced without delay by making reasonable efforts<sup>30</sup>. For this purpose, the Person with Specific Obligations must determine which official updated data concerning sanctions of competent authorities the employees must follow as well as determine the adequate frequency of checking the respective updates. The Person with Specific Obligations also defines the competent persons who can make changes to the lists and ensures that only qualified employees with the relevant rights can add or remove lists or inputs to lists.

The sanctions lists used for screening by the Person with Specific Obligations also include information disclosed by competent authorities and collected by the Person with Specific Obligations themselves on the basis of the Know-Your-Client principle, which helps them better identify the subject of sanctions, the transaction that breaches the sanction or a high sanction risk.

Lists prepared by third parties may also be used for screening if (i) in the case of outsourcing, the rules for outsourcing set out in the FSA Outsourcing Guidelines and the EBA Guidelines on Restrictive Measures are guaranteed; (ii) it is ensured that legally binding lists of sanctions are accurate and updated immediately; and (iii) the Person with Specific Obligations has made reasonable efforts to assess the quality of the respective service using the best professional skills. Screening technology requires constant calibration, validation and improvement in order to ensure efficient data screening. For this purpose, the Person with Specific Obligations establishes and implements an internal control system to avoid internal and external removal, stripping and other

---

<sup>29</sup> A false negative match is (i) a match that is identified during the screening process as a possible warning message, but is not assessed and analysed, although it is actually a correct match to the sanctions list; or (ii) when an actually correct match to the sanctions list is not identified with the screening process as a result of the incorrect calibration of the system, e.g. a correct match was not identified because the screening threshold was too high.

<sup>30</sup> According to the interpretation of the FATF, the assets of a subject of a targeted financial sanction are frozen without delay, ideally a couple of hours after the person or entity is added to the sanctions list. See The FATF Recommendations 2012 (last updated in June 2025). Online: <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>. (23.10.2025)  
Updating the lists must be based on the principles of reasonableness and best efforts, i.e. the Person with Specific Obligations makes reasonable efforts to ensure that the sanction lists used by the Person with Specific Obligations are kept relevant and updated.

manipulation of important data. More attention must thereby be paid to the part of the transaction process where the client or an employee of the organisation can manipulate the information used for screening.

The appropriate independence of checks from the risk assessment and client risk should be ensured when client data are screened in the AST.

The Person with Specific Obligations ensures that all screening technology and system calibrations, changes, updates and testing results are documented and retained, and makes them accessible to the competent authority if necessary.

### **Assessment of warning messages arising from screening technology**

Each warning message created by the AST and its matches must be assessed and a final decision on further action must be made. Using the four-eyes principle<sup>31</sup> is recommended in the case of transactions with a high risk of financial sanctions or proliferation financing.

The Person with Specific Obligations documents the results of the monitoring and screening of clients and transactions, including incorrect and true matches, and the data on the basis of which the decision was made. This activity makes it possible to analyse the screening results and ensure reporting on the efficiency, trends, typologies and functioning of the monitoring and screening system to the management.

### **Measures applied in parallel with screening technology**

The Person with Specific Obligations takes into consideration that automatic screening is not a sufficient due diligence measure for the management of financial sanction risks, including proliferation financing and evasion risks and the prevention of breaches. Therefore, the Person with Specific Obligations must also apply other and more extensive due diligence measures in the case of clients and transactions with a high financial sanction risk, such as an analysis of the risks associated with the client and the transaction.

In the case of the AST or another outsourced service, the activities and processes must be documented, including the activities of the subcontracting company, regular testing and inspections. In the case of large-scale subcontracting, the termination of the subcontracting agreement or prevention thereof must be defined in order to ensure the continuity and quality of the outsourced activities and processes. Responsibility for the outsourced service and processes that ensure compliance and the performance of the obligation to apply a financial sanction remains with the Person with Specific Obligations.

A Person with Specific Obligations who intermediates transactions (correspondent institution) must adopt reasonable solutions to identify high-risk transactions where there is no information on the initiator or payee of the payment. Such measures should be in compliance with the principles of processing payments and the principles set out in Regulation (EU) 2023/1113 of the European Parliament and of the Council.

### **Testing**

The Person with Specific Obligations carries out regular and needs-based tests in order to check that the AST is functioning efficiently and to manage the identified risks.

Testing of the AST must be supported by metrics, analysis and reporting that would make it possible to identify the emergence of a financial sanction, technology and operational risks and the occurrence of risks arising from data quality.

---

<sup>31</sup> The four-eyes principle or two-man rule is the requirement that two people must agree to acts before they are performed.

Thorough, independent and objective testing or the audit function ensure that the Person with Specific Obligations is aware of where and how their systems work and when they should be updated, supplemented or reconfigured so that they comply with the risk assessment and the indicators set out in the sanction regimes.

In order to apply the foregoing, the Person with Specific Obligations follows the EBA Guidelines on Restrictive Measures and also:

- ensures that the person who carries out the testing or the audit is impartial and independent and has the required powers, skills, experience and resources;
- ensures that if the result of the testing or the audit is not as expected, immediate effective measures are taken to identify and implement compensation measures until the root cause of the system weakness can be identified and risks can be mitigated and managed;
- documents the structure of its AST in order to clearly understand whether the risks arising from the activities of the Person with Specific Obligations have been identified and managed, including demonstrates the transparency of system bottlenecks and other measures (e.g. the risks are mitigated with other due diligence measures);
- implements an independent risk-based testing system to ensure that the AST generates high-quality warning messages, including matches, which correspond to the risk appetite.

Independent testing is carried out by qualified staff with the relevant technological experience or the independent employees of the Compliance Department of the Person with Specific Obligations, or a third party acting for this purpose or a combination thereof.

Testing may include at least the following:

- Exact match – the full name is tested against the list. This not only tests the process of match generation but also the data flow to ensure that a match is generated in respect of all data sources.
- Phonetic similarity – names that sound similar (e.g. Graig or Greig) are tested.
- Missing or added characters – tested when spaces, dashes or symbols have been added or removed. Such situations may arise, for example, if a name not in the Latin alphabet is changed into a name in the Latin alphabet. Such testing is important to make sure that the IT system is able to identify differences in punctuation marks, missing components or letters.
- Incorrect data fields – the creation of a match is tested if data have been entered in incorrect data fields or if the data fields have changed during the transport of data from one system to another.
- Spelling differences – it is tested whether there are differences in the same or similar names (e.g. Aleksey or Alexei).
- Titles or honorary titles – it is tested whether systems identify names if titles or honorary titles have been added to the names (e.g. Lord or Mr).
- The first name and surname have been swapped – tested when the first name and surname have been swapped in the data.
- Different languages – it is tested whether the system identifies names in their native language (e.g. Jüri vs Jyri).

## Finantsinspektsioon

- Identification of aliases<sup>32</sup> – it is tested how systems use variations of aliases. Whether aliases are identified and how they are handled according to the risk appetite.
- Noise simulation – it is tested whether the systems identify a match if a character is added, replaced or changed. For example, if 0 is used instead of the letter O etc.

The Person with Specific Obligations analyses the test results and assesses how to improve their systems in the light of the weaknesses identified. According to this, the employee who verifies the testing results makes a proposal for updating or changing the systems. Significant weaknesses and deficiencies identified during testing will be reported to the management board and corrective action will not be delayed. In particular, weaknesses that affect the functioning of the system to an extent that may prevent the Person with Specific Obligations from fulfilling its legal obligations, e.g. where the weakness is not mitigated by other measures, are relevant.

---

<sup>32</sup> Alias, 'aka' in English.

## **Annex 2 – Assessment of risks related to evasion and breaches of sanctions specific to Estonia**

This Annex is based on different threat assessments, typologies<sup>33</sup>, data accessible to the FSA, statistics, observations made during on-site inspections, and special information. This takes into account the services and products offered by financial institutions and their volumes as well as the geographic location of Estonia.

Some of the indicators listed in this Annex may also occur individually or together in ordinary or legitimate transactions, which is why the non-exhaustive list provided must be taken as a list that helps to identify related risks. The list of ways of evasion of financial sanctions and breaching a sanction and risk indicators given herein is not exhaustive.

The Person with Specific Obligations must make a decision on whether to request additional data and whether it is necessary proportionally and on the basis of risks, including its risk appetite. However, if the Person with Specific Obligations identifies a situation that could give rise to a sanction and the suspicion is not dispelled by the application of due diligence measures, the obligation to apply a sanction applies in any event.

This annex sets out some of the risks characteristic of financial sanctions and methods of evasion. They may be similar to the risks and methods related to money laundering and terrorist financing<sup>34</sup>, including concealing the beneficial owner and the countries where the risk of money laundering and terrorist financing and financial sanctions is high. Regions and countries where the legal framework to combat financial crime is inadequate and supervision is insufficient are also similar. However, the risks characteristic of financial sanctions and suitable methods must be taken into consideration in the risks related to money laundering and terrorist financing, and in using the methods for managing them.

It is important that warning signs cannot always be taken individually and separately. The relevant warning signs are viewed and assessed with other warning signs. The client, their activities and the region in which the client operates or whether the goods and services are purchased or sold must be taken into account among other things.

Subjects of financial sanctions rarely appear among the parties to the transaction, if at all. Instead, they use complex schemes and shell companies to hide their participation. The main breaches and evasions of financial sanctions take place with the help of third parties and intermediaries. Therefore, it is necessary for Persons with Specific Obligations to be aware of and keep themselves up to date on the risks and typologies related to financial sanctions and proliferation financing. In risk management, it is particularly important to take into account, inter alia, the typologies and analyses published by the Financial Intelligence Unit both periodically in its yearbook and on its website (fiu.ee).

The screening system can be manipulated in at least two ways:

- External evasion – the client or a third party related to them violates a financial sanction. This means that an external party removes or does not forward important data related to a transaction. Such removal or non-transmission of data is aimed at concealing the identity or

---

<sup>33</sup> Pursuant to clause 54 (1) 2) of the MLTFPA, the duties of the Financial Intelligence Unit include, among other things, strategic analysis that covers the risks, threats, trends, patterns and methods of the operation of money laundering and terrorist financing. In relation to this, the Financial Intelligence Unit, which is the competent authority in respect of financial sanctions under § 11 (3) 3) of the ISA, also makes typology announcements on financial sanctions on its website [www.fiu.ee](http://www.fiu.ee), the objective of which is to give the market guidelines for the identification of threats with the help of the described factors. Therefore, these Guidelines should be read in conjunction with the typology announcements and other timely and relevant information published by the Financial Intelligence Unit.

<sup>34</sup> See the Advisory AML Guideline of the Financial Supervision Authority. Online: [https://www.fi.ee/sites/default/files/2024-06/Finantsinspektsiooni%20rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20juhend\\_0.pdf](https://www.fi.ee/sites/default/files/2024-06/Finantsinspektsiooni%20rahapesu%20ja%20terrorismi%20rahastamise%20t%C3%B5kestamise%20juhend_0.pdf). (17.10.2025)

jurisdiction of the payer and/or payee as well as the origin or destination of the goods or service. Sanctioned persons may also use the accounts of family members or persons close to them for concealment.

- Internal evasion – the employees of the organisation commit a breach. For example, they remove important data related to a transaction or the employee fails to apply due diligence measures or there is a situation where, for example, client accounts are used to hide the origin of assets.

**Sanction risks and ways to evasion may be related to, inter alia:**

- Concealment of identity – different names and fronts are used;
- Concealment of the beneficial owner – for example, companies with complex (ownership) structures;

Various factors that increase and decrease risks also play a role in the assessment of this risk.

For example, the following factors can reduce risk:

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

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

- a single person's signature rights and the general or special powers of third parties;
  - structures established by third parties;
  - the involvement of countries with which the Person with Specific Obligations has no experience;
  - recently established business relationships;
  - few client contacts;
  - unclear objective or economically questionable structure;
  - deviation from the client's previously known needs (see business profile), i.e. unusual and incomprehensible structuring.
- Manipulation of transaction data;
  - Use of different payment channels – in particular payment channels that allow anonymity;
  - High-risk jurisdictions;
  - In a company with complex ownership structures.

**Warning signs of transactions related to activity-based financial sanctions and evasion methods may be, among other things:**

- Concealment of identity. Provision of false or incorrect information about the recipient or sender of the goods.
- It is concealed that the goods in question are restricted. The client doesn't want to provide information about the end-user of the goods.
- A shell company is used. The goods or services do not correspond to the company's business activities. The company has little or no business background. The company does not know the goods or services but still wants to buy or sell them.

- A client engaged in trading, intermediation or intermediation services and in business activities that are contrary to usual business practices at the same time, or there are significant and illogical changes in the client's business activities.
- Concealment of the end-user, final destination, reloading or both: the delivery dates are vague or deliveries are planned from outside the destination. The forwarding company is listed as the end-user or destination of the product. The manner of shipping is unusual for the product or destination. The client is evasive or non-specific when asked to explain whether the goods are meant for local use, export or re-export.
- The supply chain of the goods or services is unreasonable for the specific goods.
- Pseudonyms and forged documents are used to conceal the participation of the subject of sanctions.

Common methods used to breach and evade sanctions also include:

- Bank accounts held by citizens of a state with a high risk of sanctions or proliferation financing who act on behalf of the subject of sanctions;
- use of a joint venture where one of the owners is a subject of sanctions;
- use of the bank accounts of diplomatic employees for the benefit of subjects of sanctions;
- Cyberattacks are organised against financial institutions, including crypto service providers<sup>35</sup>, to obtain funds and evade sanctions.

**In addition to the above, the Person with Specific Obligations will take into account internationally published information, including the threat indicators specified by the FATF, when preventing proliferation financing<sup>36</sup>.**

---

<sup>35</sup> The risks of crypto asset service providers (CASPs) also include the risks of virtual asset service providers (VASPs).

<sup>36</sup> The FATF report on Complex Proliferation Financing and Sanctions Evasion Schemes (June 2025). Online: <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Complex-PF-Sanctions-Evasions-Schemes.pdf.coredownload.inline.pdf>. (13.11.2025)