Regulations and guidelines 1/2022

Draft/Preventing Money Laundering and Terrorist Financing

J. No
FIVA 23/01.00/2021

Issued
[1.9.2022]

Valid from
[1.10.2022]

Further information from
Digitalisation and Banking Service/Anti Money Laundering

FINANCIAL SUPERVISORY AUTHORITY
tel. +358 9 183 51
firstname.surname@fiva.fi
fin-fsa.fi

FIN-FSA
FINANCIAL SUPERVISORY AUTHORITY

Legal nature of regulations and guidelines

Regulations

Financial Supervisory Authority (FIN-FSA) regulations are presented under the heading ‘Regulation’ in FIN-FSA's regulations and guidelines. FIN-FSA regulations are binding legal requirements that must be complied with.

FIN-FSA issues regulations only by virtue of and within the limits of legal provisions that entitle it to do so.

Guidelines

FIN-FSA interpretations of the contents of laws and other binding provisions are presented under the heading ‘Guideline’ in FIN-FSA's regulations and guidelines.

Also recommendations and other operating guidelines that are not binding are presented under this heading, as are FIN-FSA’s recommendations on compliance with international guidelines and recommendations.

The formulation of the guideline shows when it constitutes an interpretation and when it constitutes a recommendation or other operating guideline. A more detailed description of the formulation of guidelines and the legal nature of regulations and guidelines is provided on the FIN-FSA website.

fin-fsa.fi > Regulation > Legal framework of FIN-FSA regulations and guidelines

Contents

1 Scope of application

1.1 Scope of application

These regulations and guidelines are applicable to the following obliged entities as referred to in section 1(4)(1)(5) of the Act on Preventing Money Laundering and Terrorist Financing (444/2017) (hereinafter the AML Act):

- a credit institution or branch of a third country credit institution as referred to in the Credit Institutions Act (1055/2016)
- an insurance company or special purpose vehicle as referred to in the Insurance Companies Act (521/2008)
- an employee pension insurance company as referred to in the Act on Employee Pension Insurance Companies (354/1997)
- a branch of a third country insurance company as referred to in the Act on Foreign Insurance Companies (398/1995)
- a fund management company as referred to in the Act on Common Funds (213/2019) and a depository authorised under the said Act
- an investment firm and branch of a third country firm as referred to in the Investment Services Act (747/2012)
- a central securities depository as referred to in the Act on the Book-Entry System and Settlement Activities (348/2017), including a registration fund and settlement fund established by such
- a Finnish central counterparty as referred to in the Act on the Book-Entry System and Settlement Activities
- a payment institution as referred to in the Payment Institutions Act (297/2010)
- an alternative investment fund manager with authorisation as an alternative investment fund manager under the Act on Alternative Investment Fund Managers (162/2014), or a depositary authorised under the said Act
- an entity as referred to in Article 27(2) of Regulation (EU) 2017/2402 of the European Parliament and of the Council laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation, and amending Directives 2009/65/EC, 2009/138/EC and 2011/61/EU and Regulations (EC) No 1060/2009 and (EU) No 648/2012, hereinafter referred to as Securitisation Regulation, which has been granted authorisation as referred to in Article 28 of the said Regulation
- a holding company that has been granted authorisation to pursue holding company activities as stipulated in chapter 2a of the Credit Institutions Act
- an approved public arrangement as referred to in Article 2(1)(34), and an approved reporting mechanism as referred to in Article 2(1)(36), of Regulation (EU) No 600/2014 on markets in financial instruments and amending Regulation (EU) No 648/2012, hereinafter referred to as EU Markets in Financial Instruments Regulation, that the Financial Supervisory Authority has granted authorisation and for the supervision of which it is responsible under Article 27b(1), second paragraph of the said Regulation
- a branch of a foreign entity corresponding to the abovementioned supervised entities

- a foreign entity corresponding to the abovementioned supervised entities, where the entity provides services in Finland through a representative without establishing a branch
- a financial institution belonging to the same consolidation group with a credit institution as referred to in the Credit Institutions Act
- an account operator as referred to in the Act on the Book-Entry System and Clearing Operations and a foreign corporation's Finnish office which has been granted the rights of an account operator
- a natural person and a legal person as referred to in sections 7, 7a and 7b of the Act on Payment Institutions and an alternative investment fund manager under the registration obligation pursuant to in the Act on Alternative Investment Fund Managers
- a local mutual insurance association as referred to in the Local Mutual Insurance Associations Act (1250/1987)
- an insurance intermediary and ancillary insurance intermediary as referred to in the Insurance Distribution Act (234/2018), and a branch of a foreign insurance intermediary and foreign ancillary insurance intermediary operating in Finland
- a crowdfunding intermediary as referred to in the Crowdfunding Act (734/2016)[1];
- a Finnish credit intermediary as referred to in the Act on Intermediaries of Consumer Credit Relating to Residential Property (852/2016) and a Finnish branch of a foreign credit intermediary
- a virtual currency provider as referred to in the Act on Virtual Currency Providers (572/2019).

1.2 Definitions

For the purposes of these regulations and guidelines, the following definitions shall apply:

Customer refers to a natural or legal person to which the supervised entity provides services.

Customer relationship refers to a contractual relationship, based on which the supervised entity provides services to a customer and which is:

- assumed, at the inception of the contractual relationship, to be permanent or become permanent regardless of the initial term of the contractual relationship or
- deemed permanent based on an assessment of the frequency, regularity of duration of separate transactions or other relevant factors based on a risk-based assessment of the obliged entity.

Customer due diligence refers to the measures provided in chapter 3 of the AML Act, and it includes the following duties:

- customer identification and identity verification (including the identification, verification of identity, and ascertaining of the right of representation of the customer's representative),
- collection of information on the customer in order to know the customer and their activities (including the obligation to know the beneficial owners), and

[1] *see Government Bill 228/2021*

- ongoing monitoring of the customer relationship and obligation to obtain information.

Supervised entity refers to obliged entities under the AML Act which are supervised by the FIN-FSA pursuant to chapter 7, section 1(1)(1) of the AML Act.

Compliance function refers to a part in the supervised entity's organisation whose function is to supervise compliance with legal requirements and internal guidelines, to assess the adequacy of actions proposed to prevent and remediate any detected shortcomings in regulatory compliance and to provide support and advice on compliance with regulation and internal guidelines to the management and other staff of the supervised entity. It may also prepare policies and processes to manage risks pertaining to compliance with applicable requirements (so-called compliance risks) and to ensure regulatory compliance.

2 Legislative background and international recommendations

2.1 Legislation

The following legal provisions relate to the matters addressed in these regulations and guidelines:

- AML Act (note! New provisions or those proposed for amendment in the Government bill 236/2021 and their justifications are highlighted in blue for clarity).
- Act on Detecting and Preventing Money Laundering and Terrorist Financing (503/2008, hereinafter referred to as the old AML Act)
- Act on the Financial Intelligence Unit (445/2017)
- Act on the Bank and Payments Account Monitoring System (571/2019)
- Act on Virtual Currency Providers (572/2019)
- Act on Insurance Companies (521/2008)
- Act on the Financial Supervisory Authority (878/2008, hereinafter the FIN-FSA Act)
- Credit Institutions Act (610/2014)
- Investment Services Act (747/2012)
- Act on Common Funds (213/2019)
- Act on Payment Institutions (297/2010)
- Act on Alternative Investment Fund Managers (162/2014 (hereinafter the AIFM Act)
- Crowdfunding Act (734/2016)
- Act on Intermediaries of Consumer Credit Relating to Residential Property (852/2016)
- Act on the Book-entry System and Clearing Operations (348/2017)
- Act on Strong Electronic Identification and Electronic Trust Services (617/2009)
- Consumer Protection Act (38/1978)
- Credit Information Act (527/2007)
- Act on the Amalgamation of Deposit Banks (599/2010)
- Guardian Services Act (442/1999)
- Data Protection Act (1050/2018)
- Government Decree on Prominent Public Functions Referred to in the Act on Preventing Money Laundering and Terrorist Financing (610/2019)

- Government Decree on Customer Due Diligence Procedures and Anti-Money Laundering and Counter-Terrorist Financing Risk Factors (929/2021)

2.2 European Union Regulations

The following directly applicable European Union Directives are related to the matters addressed in these regulations and guidelines:

- Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (*Payer Information Regulation*)
- Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries
- Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies[2]

2.3 European Union Directives

The following European Union Directives are related to the matters addressed in these regulations and guidelines:

- Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (hereinafter *Fifth Anti-Money Laundering Directive*)
- Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (hereinafter *Fourth Anti-Money Laundering Directive*, 4AMLD)

2.4 FIN-FSA's regulatory powers

FIN-FSA's power to issue binding regulations is based on the following legal provisions:

- Chapter 9, section 6 of the AML Act
- Section 39, subsection 4 of the Payment Institutions Act.
- Chapter 15, section 18, subsection 4 of the Credit Institutions Act
- Section 13, subsection 4 of the Virtual Currency Providers Act

[2] *See up-to-date valid list of high-risk third countries in Annex of the Regulation.*

- Chapter 12, section 3, subsection 4 of the Investment Services Act
- Chapter 12, section 10 of the AIFM Act
- Chapter 6, section 21, subsection 1, paragraph 4 of the Insurance Companies Act.
- Chapter 26, section 15, subsection 4 of the Act on Common Funds
- Chapter 8, section 13 of the Act on the Book-Entry System and Settlement Operations
- Section 17, subsection 3 of the Act on the Amalgamation of Deposit Banks

2.5 International recommendations

The following guidelines and recommendations issued by the European Banking Authority (EBA) are related to the matters addressed in these regulations and guidelines:

- Guidelines on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (hereinafter *the EBA Risk Factors Guidelines*) under Articles 17 and 18(4) of Directive (EU) 2015/849 repealing and replacing the Guidelines JC/2017/37 (issued on 3 March 2021) (EBA/GL/2021/02), available at Finanssivalvonta.fi
- EBA Guidelines on internal governance (EBA/GL/2021/05)[3], available at Finanssivalvonta.fi
- EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02), available at Finanssivalvonta.fi

Other international guidelines and recommendations related to the matters addressed in these regulations and guidelines:

- The European Commission's Supranational risk assessment of the money laundering and terrorist financing risks affecting the Union (hereinafter *the Supranational Risk Assessment*) (published on 24 June 2019)
- Financial Action Task Force (hereinafter *FATF*) Guidance on Digital ID (2020)
- International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations 2012 - amended June 2021

[3] *FIN-FSA regulations and guidelines 14/2021*

3 Objectives

(1) The objective of these regulations and guidelines is to provide entities supervised by the FIN-FSA with interpretations and recommendations on the application of regulation concerning the prevention of money laundering and terrorist financing (AML/CFT).

(2) Another objective of these regulations and guidelines is to issue binding regulations to supervised entities pursuant to the regulatory powers laid out in the AML Act and above in chapter 2.4.

(3) The objective of these regulations and guidelines is to guide supervised entities in their AML/CFT measures and thereby combat the use of the financial system in money laundering and terrorist financing.

(4) These regulations and guidelines seek to guide supervised entities in taking proportionate and risk-based actions against money laundering and terrorist financing to the extent legislation does not provide adequate guidance. A further intention is to harmonise and improve the effectiveness of application of regulation concerning the prevention of money laundering and terrorist financing.

(5) At the same time, the FIN-FSA's regulations and guidelines are also renewed and brought up to date in this topic area.

4 Risk assessment

4.1 General

(1) The FIN-FSA has issued regulations and guidelines 7/2021, recommending compliance with the EBA Risk Factors Guidelines (EBA/GL/2021/02).

GUIDELINE (paragraph 2)

(2) The FIN-FSA recommends that also other supervised entities than those falling within the scope of application of regulations and guidelines 7/2021 comply with the EBA Risk Factors Guidelines.

4.2 Purpose and content of the risk assessment

(3) In accordance with chapter 2, section 3 of the AML Act, entities under the notification obligation (hereinafter 'obliged entities') shall make a risk assessment to identify and evaluate the risks of money laundering and financing of terrorism. In conducting the risk assessment, the nature, size and extent of the obliged entity's activities shall be taken into account.

(4) The FIN-FSA's authority to issue more detailed regulations on the management of risks posed by customers to the activities of a supervised entity is based on the following provisions: Section 39(4) of the Payment Institutions Act, chapter 15, section 18(4) of the Credit Institutions Act, section 13(4) of the Virtual Currency Providers Act, chapter 12, section 3(4) of the Investment Services Act, chapter 12, section 10 of the AIFM Act, chapter 6, section 21(4) of the Insurance Companies Act, chapter 26, section 15(4) of the Act on Common Funds and chapter 8, section 13 of the Act on the Book-Entry System and Settlement Operations.

(5) For the purposes of regulations 7–14, a supervised entity refers to supervised entities falling within the scope of authority to issue regulations under paragraph 4 above.

GUIDELINE (paragraph 6)

(6) According to the Government bill[4] the obliged entity's own risk assessment helps the obliged entity to plan a risk-based approach to its activities and functions as evidence for supervisory authorities of the rationale applied by the obliged entity for example when opting for simplified or enhanced customer due diligence in individual cases.

REGULATION (paragraphs 7–14)

(7) A supervised entity's risk assessment shall present the supervised entity's justified view of how the products and services provided by it can be utilised in money laundering.

(8) A supervised entity's risk assessment shall present the supervised entity's justified view of how the products and services provided by it can be utilised in financing terrorism.

(9) Supervised entities shall identify the money laundering and terrorist financing risk factors related to their new and existing customers, countries and geographical areas as well as products,

[4] *Government bill 228/2016, p. 101.*

services, distribution channels and technologies that are new, in development or already existing. The impact of these risk factors must be assessed.

(10) Supervised entities shall prepare the risk assessment by reviewing the risk pertaining to each product and service separately.

(11) In its risk assessment, a supervised entity shall describe the management methods applied by it to money laundering and terrorist financing (ML/TF) risks, and assess their impact on the risk factors identified.

(12) The risk assessment shall include a justified assessment of the remaining risk (residual risk) and of whether the residual risk corresponds to the supervised entity's risk appetite or whether it should take requisite actions to mitigate and manage residual risk.

(13) A supervised entity shall prepare a long-term risk appetite statement, i.e. a decision on the limits of ML/TF risks accepted by the supervised entity in its activities, with a view to other requirements pertaining to for example capital adequacy and risk management as well as other regulation. The extent and level of detail of the risk appetite statement shall be proportionate with the size of the supervised entity and the nature and extent of its activities.

(14) The risk appetite statement shall be approved by the body referred to in chapter 2, section 3(3) of the AML Act.

GUIDELINE (paragraphs 15–16)

(15) The FIN-FSA recommends that provisions 7–14 above are also complied with by supervised entities excluded from the scope of authority to issue regulations under paragraph 4.

(16) The FIN-FSA recommends that supervised entities also assess the probability of the risks identified by them in their risk assessment.

4.3 Methodology and documentation of the risk assessment

(17) In accordance with chapter 2, section 3(2) of the AML Act, the risk assessment shall always be made by taking into account the nature, size and extent of the obliged entity's activities. The obliged entity shall have in place policies, procedures and controls that are sufficient with regard to the abovementioned factors to reduce and effectively manage the risks of money laundering and terrorist financing.

(18) In accordance with chapter 2, section 3(1) of the AML Act, the risk assessment shall be updated on a regular basis, and any changes thereto shall be supplied without undue delay to the supervisory authority at its request.

(19) The FIN-FSA's authority to issue more detailed regulations on the management of risks posed by customers to the activities of a supervised entity is based on the following provisions: Section 39(4) of the Payment Institutions Act, chapter 15, section 18(4) of the Credit Institutions Act, section 13(4) of the Virtual Currency Providers Act, chapter 12, section 3(4) of the Investment Services Act, chapter 12, section 10 of the AIFM Act, chapter 6, section 21(4) of the Insurance Companies Act, chapter 26(15)(4) of the Act on Common Funds and chapter 8, section 13 of the Act on the Book-Entry System and Settlement Operations.

(20) For the purposes of regulations 21–25, a supervised entity refers to supervised entities falling within the scope of authority to issue regulations under paragraph 20 above.

REGULATION (paragraphs 21–25)

(21) The up-to-datedness of the risk assessment shall be checked annually, and the risk assessment shall be updated where necessary. Procedures shall be in place to check the up-to-datedness, and the check shall be documented.

(22) There shall be policies and procedures to update the risk assessment, and any updates to the risk assessment as well as their justifications shall be documented.

(23) The risk assessment shall be updated whenever there are changes in the risk factors. Such changes include at least new products and services, new customer groups, expansion of services to new geographical areas or distribution channels, or changes in the technology used.

(24) The risk assessment shall also be updated whenever there are changes in the supervised entity's risk management framework or the supervised entity detects new vulnerabilities in its activities.

(25) The up-to-datedness of the risk appetite statement shall be ensured and the statement be updated if necessary in connection with the update of the risk assessment.

GUIDELINE (paragraphs 26–29)

(26) The FIN-FSA recommends that the provisions of paragraphs 21–25 above are also complied with by supervised entities excluded from the authority to issue regulations under paragraph 19.

(27) According to the FIN-FSA's interpretation, the obligation referred to in chapter 2, section 3(1) of the AML Act to prepare a risk assessment means that the risk assessment shall be documented so that it can be submitted to the FIN-FSA without undue delay.

(28) According to the FIN-FSA's interpretation, the obligation referred to in chapter 2, section 3(1) of the AML Act to prepare a risk assessment also entails that the description of the risk assessment process and the policies and procedures applied therein shall be documented so that the description can be submitted to the FIN-FSA without undue delay.

(29) The FIN-FSA recommends that supervised entities assess whether it is necessary to update the risk appetite statement in for example when they identify new risks related to their activities, revise their assessment of previously identified risks or consider that their risk management measures are no longer adequate to manage the ML/TF risks related to their activities in a proportionate way.

4.4 Sources of the risk assessment and their use

(30) In accordance with chapter 2, section 1(2) of the AML Act, the purpose of the national risk assessment is, inter alia, to provide the obliged entities with information to support the preparation of the risk assessment.

(31) In accordance with chapter 2, section 2(1) of the AML Act, the FIN-FSA shall prepare an assessment of the risks of money laundering and terrorist financing among the obliged entities

supervised by it, and according to subparagraph (4), it shall publish a summary of the risk assessment.

GUIDELINE (paragraphs 32-25)

(32) According to the Government bill,[5] the European Commission shall prepare a supranational EU risk assessment of money laundering and terrorist financing, and in doing so, take into account the view of the European supervisory authorities, national anti-money laundering units and other authorities. In their national risk assessments of money laundering and terrorist financing, the member states shall take into account the results of the Commission's risk assessment, and the obliged entities shall take both assessments into account in their assessment of the risks of money laundering and terrorist financing in their activities.

(33) The FIN-FSA recommends that, in conducting the risk assessment, supervised entities take into consideration at least:

- The summary of the FIN-FSA's supervisor-specific risk assessment
- Government Decree on Customer Due Diligence Procedures and Anti-Money Laundering and Counter-Terrorist Financing Risk Factors (929/2021)
- Annexes 2 and 3 of the Fourth Anti-Money Laundering Directive on high- and low-risk circumstances.

(34) The FIN-FSA recommends paying particular attention to paragraphs 1.29–1.32 of the EBA Risk Factors Guideline on the data sources to be used in the risk assessment.

(35) The FIN-FSA recommends that, in conducting and updating the risk assessment, supervised entities take into account and document information collected in the course of their own activities on the risks of money laundering and terrorist financing, as well as their management methods. For example, new threats or risks identified in the ongoing monitoring of customers should be taken into consideration in the context of the updating the risk assessment. At the same time, it should be assessed whether existing measures are enough to manage these new risks in a proportionate way or whether new risk management measures should be created.

[5] *Government Bill 228/2016, p. 99.*

5 Organisation of AML/CFT functions

5.1 Policies and procedures

(1) In accordance with chapter 2, section 3(2) of the AML Act, the obliged entity shall have in place policies, procedures and controls that are sufficient with regard to the abovementioned factors to reduce and effectively manage the risks of money laundering and terrorist financing. The policies, procedures and controls shall comprise at least:

1) the development of internal policies, procedures and controls;

2) an internal audit when justified with regard to the nature of the obliged entity's activities or the size of the obliged entity.

(2) In accordance with chapter 2, section 3(3) of the AML Act, the obliged entity shall prepare the policies, procedures and controls referred to in subsection 2 and shall monitor and enhance measures relating to these.

(3) In accordance with chapter 9, section 1(3) of the AML Act, obliged entities shall have in place guidelines suited to their particular activities regarding customer due diligence procedures and the obtaining of customer information, ongoing monitoring, the obligation to obtain information as well as compliance with the reporting obligation relating to the prevention of money laundering and terrorist financing.

(4) In this chapter, model risk management practices refer to manual and IT system-based processes and rules used by the supervised entity when preparing an obliged entity's risk assessment referred to in chapter 2, section 3 of the AML Act, collecting customer due diligence data referred to in chapter 3, section 3 of the AML Act, assessing the risks in a customer relationship in accordance with chapter 3, section 1(2) of the AML Act, conducting ongoing monitoring referred to in chapter 3, section 4(2) of the AML Act and seeking to detect transactions referred to in subsection 3 of said section.

(5) The FIN-FSA's authority to issue more detailed regulations on the management of risks posed by customers to the activities of a supervised entity is based on the following provisions: section 39(4) of the Payment Institutions Act, chapter 15, section 18(4) of the Credit Institutions Act, section 13(4) of the Virtual Currency Providers Act, chapter 12, section 3(4) of the Investment Services Act, chapter 12, section 10 of the AIFM Act, chapter 6, section 21(4) of the Insurance Companies Act, chapter 26, section 15(4) of the Act on Common Funds and chapter 8, section 13 of the Act on the Book-Entry System and Settlement Operations.

(6) For the purposes of regulations 13-15, a supervised entity refers to supervised entities falling within the scope of authority to issue regulations under paragraph 5 above.

GUIDELINE (paragraphs 7-12)

(7) According to the FIN-FSA's interpretation, the policies and procedures referred to in chapter 2, section 3(2) of the AML Act to reduce and manage the risks of money laundering and terrorist

financing must cover at least model risk management practices, compliance with the customer due diligence obligation, compliance with the reporting obligation and the retention of data.[6]

(8) According to the FIN-FSA's interpretation, the controls referred to in chapter 2, section 3(2) of the AML Act refer to functions whose purpose is to ensure that the supervised entity complies with AML/CFT regulation as well as the policies and procedures established by the supervised entity to reduce and manage money laundering and terrorist financing. Such functions include internal control, compliance and internal audit.

(9) According to the FIN-FSA's interpretation, the policies referred to in chapter 2, section 3(2) of the AML Act refer to high-level principles prepared in writing by the supervised entity to reduce risks and to manage them effectively in various areas of money laundering and terrorist financing, including a description of how the management of risks pertaining to money laundering and terrorist financing has been organised in practice.

(10) According to the FIN-FSA's interpretation, the procedures referred to in chapter 2, section 3(2) of the AML Act are more detailed than policies and guide the practical actions of the supervised entity in preventing money laundering and terrorist financing. Depending on the nature, size and extent of the business of the supervised entity, the policies may include guidance of different levels ranging from general guidance to detailed operative instructions.

(11) According to the FIN-FSA's interpretation, chapter 9, section 1(3) of the AML Act means that the procedures must be prepared and documented at the level of concrete operating instructions so as to create a consistent framework.

(12) According to the FIN-FSA's interpretation, under chapter 2, section 3(3) of the AML Act, supervised entities shall have procedures in place to ensure that its policies and procedures are up to date, and to develop them.

REGULATION (paragraphs 13-15)

(13) Supervised entities must prepare a description of the model risk management practices at their disposal.

(14) Supervised entities must ensure the performance of the model risk management, test them on a regular basis and update them when necessary in accordance with the policies and procedures established for this purpose.

(15) The policies and procedures established by supervised entities for the purposes of customer due diligence, compliance with the reporting obligation and retention of data must cover at least the following areas:

- risk-based assessment of the customer relationship,
- customer identification and verification of identity,
- collection of data needed for customer due diligence
- ongoing monitoring of the customer relationship and obligation to obtain information
- compliance with the reporting obligation, and

[6] *See Government bill 228/2016, p.101*

- retention of customer data and information concerning suspicious transactions.

Procedures pertaining to customers effectively also include procedures for the identification of the customers' beneficial owners in accordance with the provisions of chapter 3, section 6 of the AML Act.

GUIDELINE (paragraph 16)

(16) The FIN-FSA recommends that the provisions of paragraphs 13–15 above are also complied with by supervised entities excluded from the authority to issue regulations under paragraph 5.

5.2 Arrangement of the organisation

5.2.1 Lines of defence

(17) In this chapter, the model of three lines of defence refers to a model where a supervised entity's internal control and risk management duties are divided among the following functions:

- supervised entity's business units (first line of defence)
- risk management functions and compliance functions (second line of defence)
- internal audit (third line of defence)

GUIDELINE (paragraphs 18–19)

(18) The FIN-FSA has issued regulations and guidelines 14/2021 implementing nationally the updated EBA Guidelines on internal governance.

(19) The FIN-FSA recommends that also supervised entities outside the scope of application of regulations and guidelines referred to in paragraph 18 review the EBA guidelines on internal governance in preparing their policies, procedures and controls referred to in chapter 2, section 3(2) of the AML Act and assess whether it is appropriate to design the risk management of the supervised entity in accordance with the model of three lines of defence, with a view to the size of the supervised entity, the nature and quality of its activities and its organisational structures.

5.2.2 Management duties to prevent money laundering and terrorist financing

5.2.2.1 Approval of policies and procedures

(20) In accordance with chapter 2, section 3(3) of the AML Act, when the obliged entity is a legal person, the board of directors, active partner or other person holding an equivalent senior management position shall approve the policies, procedures and controls s to reduce and effectively manage the risks of money laundering and terrorist financing, and also monitor and enhance related measures.[7]

[7] *Article 8(5) of 4AMLD.*

GUIDELINE (paragraphs 21–23)

(21) According to the FIN-FSA's interpretation, the policies, procedures and controls referred to in chapter 2, section 3(2) of the AML Act shall be approved by the board of directors or active partner, depending on the form of incorporation.

(22) According to the FIN-FSA's interpretation, if a supervised entity does not have a board of directors or an active partner, the policies, procedures and controls referred to in chapter 2, section 3(2) of the AML Act may be approved by another person holding an equivalent senior management position.

(23) According to the FIN-FSA's interpretation, another person holding an equivalent senior management position referred to in chapter 2, section 3(3) of the AML Act refers to a person with authority to adopt the strategy, targets and general management of the supervised entity. The party approving the policies and procedures shall have sufficient information on ML/TF risks and authority to make decisions with an impact on these risks. For example, the country manager of the branch of a foreign company may be considered a person holding an equivalent senior management position.

5.2.2.2 Designated responsible person from the management

(24) Chapter 9, section 1 of the AML Act provides that obliged entities shall designate a person from their management to be responsible for supervising compliance with said Act and provisions issued under it.[8]

GUIDELINE (paragraphs 25–28)

(25) The FIN-FSA has issued regulations and guidelines 14/2021, recommending compliance with the EBA Guidelines on internal governance (GL/2021/05).

(26) The FIN-FSA has issued regulations and guidelines 15/2021, recommending compliance with the EBA and ESMA Guidelines on the assessment of the suitability of members of the management body and key function holders (EBA/GL/2021/06 and ESMA35-36-2319).

(27) According to the FIN-FSA's interpretation, management as referred to in chapter 9, section 1(1) of the AML Act among which a responsible person shall be designated to ensure compliance with this Act and the provisions issued thereunder, refers to the board of directors, the managing director, active partner or another person holding an equivalent senior management position depending on the form of incorporation. For example, the country manager of the branch of a foreign company may be considered a person holding an equivalent senior management position. The designated person shall have adequate knowledge of the MF/TF risks posed to the supervised entity and adequate authority to make decisions concerning the risks posed to the supervised entity.

(28) According to the FIN-FSA's interpretation, the designation of the person referred to in chapter 9, section 1(1) of the AML Act does not constitute an exception to provisions laid out elsewhere in legislation concerning the responsibility of the management.[9] The purpose of the regulation is to

[8] *Article 46(4) of 4AMLD.*
[9] *EBA Guideline on internal governance (GL/2021/05), paragraph 31.*

ensure that there is a person in the management with an adequate understanding of the prevention of money laundering and terrorist financing and who acts as the contact person for the person responsible for compliance as referred to in the AML Act (see section 5.2.3).

5.2.3 Person responsible for compliance

(29) In accordance with chapter 9, section 1(1) of the AML Act, obliged entities shall also designate a person to be responsible for internal supervision of compliance with said Act and the provisions issued under it, providing this is justified with regard to the size and nature of the obliged entity.

GUIDELINE (paragraphs 30–35)

(30) According to the FIN-FSA's interpretation, the reference in chapter 9, section 1(1) of the AML Act to the internal supervision of compliance with said Act and the provisions issued under it means the compliance function, and the person to be responsible for internal supervision of compliance with said Act and the provisions issued under it means the appointment of a compliance officer who shall be responsible for monitoring compliance with AML/CFT legislation as well as with the obliged entity's own policies and procedures.

(31) Paragraphs 204–213 of the EBA Guidelines on internal governance provide detailed guidelines on the organisation of the compliance function for supervised entities falling within the scope of the EBA Guidelines.

(32) The FIN-FSA recommends that the compliance officer is appointed at a sufficiently high level within the organisation, so that he or she has the authority to report any findings directly to the party referred to above in section 5.2.2.2 (designated responsible person from the management) and submit such findings and suggestions for review by the party referred to above in section 5.2.2.1. Where justified considering the nature and size of the business, the compliance officer should be designated at the management level[10].

(33) According to the FIN-FSA's interpretation, in assessing whether they should designate at person referred to in chapter 9, section 1(1) of the AML Act to be responsible for supervising compliance with the AML Act and provisions issued under it, supervised entities shall consider the following factors:

1. size of the organisation to be supervised;
2. whether the supervised entity operates in a sector involving a high money laundering/terrorist financing risk according to the sector-specific risk assessment made by the FIN-FSA;
3. whether the supervised entity's activities involve significant money laundering and terrorist financing risks according to its own risk assessment; and
4. Whether the appointment of an officer should be considered justified with a view to the supervised entity's risk management methods and internal control procedures.

(34) The FIN-FSA recommends supervised entities to ensure that adequate resources are in place for the conduct of compliance duties, and if the compliance officer also has other duties, to ensure that such duties are not in conflict with the principles concerning the independence of the compliance function. In accordance with the principles requiring independence, people working in

[10] *Article 8(4 a) of 4AMLD.*

the compliance function should be independent of the business areas and internal units supervised by them.

(35) The FIN-FSA recommends supervised entities to ensure that responsibility for the performance of compliance duties remains on the person designated as the compliance officer also in circumstances where the compliance officer delegates duties belonging to him or her to subordinates.

5.2.4 Internal audit

(36) In accordance with chapter 2, section 3(2)(2) of the AML Act, the policies, procedures and control of an obliged agent shall include internal audit, where it is justified with a view to the size of the obliged agent and the nature of its activities.

GUIDELINE (paragraphs 37–39)

(37) According to the Government bill[11] obliged agents should ensure that their internal audit or another comparable function tests the policies and procedures.

(38) According to the FIN-FSA's interpretation, the purpose of an internal audit referred to in chapter 2, section 3(2)(2) of the AML Act is to independently supervise and inspect the compliance of the activities of the supervised entity with the law and whether the supervised entity complies with its own policies and procedures.

(39) According to the FIN-FSA's interpretation, the arrangement of an internal audit referred to in chapter 2, section 3(2)(2) of the AML Act is always justified if the legislation applying to the supervised entity requires the arrangement of an internal audit. In this case, the auditing of the AML/CFT functions shall be part of the internal audit's duties.

5.3 Policies and procedures concerning employees

5.3.1 Background checks of employees

GUIDELINE (paragraphs 40–43)

(40) The FIN-FSA recommends that supervised entities' policies and procedures referred to in chapter 2, section 3(2) of the AML Act cover the background checks of personnel working in the AML/CFT functions. The purpose of the background check is to ensure that supervised entities' employees do not abuse their position for money laundering and/or terrorist financing purposes.

(41) The FIN-FSA recommends supervised entities to ensure that the policies and procedures concerning background checks on employees must be commensurate with the nature, size and extent of the obliged agent's activities and the ML/TF risks involved.

(42) The FIN-FSA recommends that supervised entities conduct the background checks on a risk-sensitive basis, taking into consideration how critical the employee's role is for the prevention of money laundering and terrorist financing and that employee background checks have impacts limiting privacy and the protection of personal data as referred to in section 10 of the Constitution.

[11] *Government bill 228/2016, p.101.*

(43) The FIN-FSA recommends supervised entities to note that the background check does not mean a background check by the Finnish Security and Intelligence Service under the Security Clearance Act (762/2014) or a background check referred to in Criminal Records Act (770/1993) but such lighter procedures whereby it is ensured that employees meet, in the context of recruitment and on an ongoing basis, any requirements posed to their professional competence, such as formal qualification, adequate education and experience. In the context of recruitment, the background check would entail, for example, the verification of information provided by the employee, to be conducted by contacting previous employers and educational institutions, subject to the employee's permission. The quality and extent of the background could vary depending on the duties assigned to the employee. The principal purpose would be to ensure that the person's education, professional experience, personal characteristics and ability meet the requirements of the position.

5.3.2 Training and competence of employees

(44) In accordance with chapter 9, section 1(1) of the AML Act, obliged entities shall ensure that their employees are provided with training to ensure compliance with this Act and the provisions issued under it.

GUIDELINE (paragraphs 45–47)

(45) According to the FIN-FSA's interpretation, the obligation under chapter 9, section 1(1) of the AML Act to ensure that employees are provided with training means that supervised entities shall prepare policies and procedures for training and supervise compliance with them by keeping records of the timing, content and participants of training, among other things.

(46) According to the FIN-FSA's interpretation, training given to ensure compliance with the obligation under chapter 9, section 1(1) of the AML Act shall be detailed enough to ensure that supervised entities' employees have the capability to perform on their duties in line with the requirements of the supervised entities' policies and procedures. The fulfilment of the obligation may require the preparation of separate training plans for different groups of employees.

(47) The FIN-FSA recommends supervised entities to ensure the continuous maintenance of professional competence of their employees during the employment relationship to an extent required by the duties by monitoring of the adequacy and up-to-datedness of the training.

5.3.3 Protection of employees

(48) In accordance with chapter 9, section 1(2) of the AML Act, obliged entities shall take steps to protect employees who submit reports on suspicious transactions as referred to in chapter 4, section 1 of said Act.

(49) Chapter 4, section 4 of the AML Act provides on the secrecy obligation concerning suspicious transactions.

GUIDELINE (paragraphs 50–52)

(50) According to the FIN-FSA's interpretation, the purpose of the obligation under chapter 9, section 1(2) of the AML Act is to protect those reporting suspicious transactions internally or to the

Financial Intelligence Unit from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.[12]

(51) According to the FIN-FSA's interpretation, compliance with the obligation provided in chapter 9, section 1(2) of the AML Act requires supervised entities to have procedures in place to protect employees making reports under chapter 4, section 1 of the AML Act, to assess and develop the adequacy of said procedures and to monitor compliance with them.

(52) The FIN-FSA recommends supervised entities to assess whether also other employees than those making reports under chapter 4, section 1 of the AML Act working in its functions may be exposed to threats or hostile action, and where necessary, create procedures to protect them. Such employees could include, for example, whose working in the customer interface or in AML/CFT functions.

5.4 Reporting of suspected violations

(53) In accordance with chapter 7, section 8(1) of the AML Act, obliged entities shall have in place procedures allowing its employees or agents to report any suspected violations of this Act and the provisions issued under it by means of an independent channel within the obliged entity (whistleblowing procedures).

(54) However, in accordance with chapter 7, section 8(1) of the AML Act, obliged entities need not have in place the procedures referred to above when the supervisory authority on the basis of the obliged entity's risk assessment decides the reporting channel of the supervisory authority to be sufficient in light of the obliged entity's size and activities and the risks of money laundering and terrorist financing associated with it.

(55) In accordance with chapter 7, section 8 of the AML Act, obliged entities shall take appropriate and adequate steps to protect whistleblowers.

(56) In this chapter, suspected violations refer to suspicions by an obliged entity's employee or representative that the AML Act or provisions and regulations issued thereunder are not complied with in the activities of an obliged entity. A suspected violation is different from a suspicious transaction report.

GUIDELINE (paragraphs 57–58)

(57) According to the FIN-FSA's interpretation, in order to comply with chapter 7, section 8 of the AML Act, supervised entities shall prepare policies and procedures for reporting and processing suspected violations, including measures to protect the reporters. The procedures shall include instructions for employees on how to report suspected violations.

(58) According to the Government bill,[13] if another Act governing the activities of an obliged entity, such as a credit institution or investment firm, provides on a corresponding system, the obliged entity may collect the data into a single system.

[12] *Article 38(1) of 4AMLD.*
[13] *Government bill 228/2016, p. 126.*

5.5 Policies and procedures of a group or another financial consortium

(59) In accordance with chapter 9, section 1(1) of the AML Act, when the obliged entity is a part of a group or other financial consortium, it shall furthermore comply with the internal policies and guidelines of the group or other financial consortium issued to ensure compliance with this Act and the provisions issued under it. These internal policies of the group or other financial consortium shall cover at least the following:

1) practices and procedures for exchange of information concerning customer due diligence and management of the risks of money laundering and terrorist financing within a group;

2) group-level orders for supervision of compliance with the regulations on intra-group exchange of information on customers, accounts and transactions, for inspection and for prevention of money laundering and terrorist financing, including information about, and an assessment of, unusual transactions or other actions;

3) sufficient measures to ensure the use and secrecy of information, including measures to safeguard the secrecy obligation referred to in chapter 4, section 4.

(60) In accordance with chapter 9, section 2(1) of the AML Act, obliged entities shall comply with the customer due diligence obligations laid down in the AML Act also at their branches located in non-EEA Member States.

(61) Chapter 9, section 2(2) of the AML Act provides that obliged entities shall ensure that the obligations laid down in the AML Act are complied with in subsidiaries located in both EEA and non-EEA Member States in which the obliged entity holds more than 50% of the votes conferred by the shares or units.

(62) In accordance with chapter 9, section 2(1) of the AML Act, an obliged entity that has places of business in other Member States shall ensure that these places of business comply with the national provisions on transposing the Anti-Money Laundering Directive into the national law of the other Member State concerned.

(63) Chapter 9, section 2(2) of the AML Act provides on procedures applying to circumstances where the legislation of the other Member State does not permit compliance with the customer due diligence procedures laid down in the AML Act.

(64) Commission Delegated Regulation (EU) 2019/758 provides on minimum actions and the additional measures that shall be taken to mitigate money laundering and terrorist financing risk in certain third countries whose law does not permit the implementation of group-wide AML/CFT of terrorism policies and procedures.

GUIDELINE (paragraphs 65–69)

(65) According to the FIN-FSA's interpretation, chapter 9, section 1(1) of the AML Act means that a group or other financial consortium shall prepare policies and procedures applying to the whole group or financial consortium on the prevention of money laundering and terrorist financing paying particular attention to the matters concerning the exchange of information and secrecy referred to in chapter 9, section 1(1) of the AML Act.[14]

[14] *Article 45(1) of 4AMLD.*

(66) According to the FIN-FSA's interpretation, chapter 9, section 1(1) of the AML Act means that if the customer due diligence obligations within the group or other financial consortium are fulfilled by another obliged entity (so-called *third party*), the policies and procedures referred to above in paragraph 65 shall include policies and procedures for the use of third parties (for more details on the use of third parties, see chapter 10).

(67) According to the FIN-FSA's interpretation, the obligation under chapter 9, section 2(2) of the AML Act to ensure subsidiaries' compliance with the AML Act only applies to subsidiaries belonging to the scope of AML/CFT regulation in Finland or the country of location.

(68) According to the FIN-FSA's interpretation, member states in chapter 9, section 2(3) of the AML Act refer to EEA member states, since all EEA member states have implemented the Fourth Anti-Money Laundering Directive into their national legislation.

(69) According to the FIN-FSA's interpretation, pursuant to chapter 9, section 2(3) of the AML Act, supervised entities shall ensure that its branches or majority-owned subsidiaries comply with the legislation of the country of location implementing the Fourth Anti-Money Laundering Directive into their national legislation particularly in circumstances where the country of location has more stringent legislation than Finland.

6 Customer due diligence

6.1 General

(1) The FIN-FSA has issued regulations and guidelines 7/2021, recommending compliance with the EBA Risk Factors Guidelines (EBA/GL/2021/02).

GUIDELINE (paragraph 2)

(2) The FIN-FSA recommends that also other supervised entities than those falling within the scope of application of regulations and guidelines 7/2021 comply with the EBA Risk Factors Guidelines also when fulfilling their obligations concerning customer due diligence.

6.2 Risk-based assessment of the customer relationship

(3) Customer due diligence is defined in chapter 1.2 of these regulations and guidelines.

(4) Chapter 3 of the AML Act provides on customer due diligence obligations.

(5) In accordance with chapter 3, section 1(2) of the AML Act, customer due diligence measures shall be observed throughout the course of the customer relationship on the basis of risk-based assessment.

(6) In order to comply with the obligation, the obliged agent shall have the policies and procedures referred to in chapter 2, section 3(2) of the AML Act in place, and they shall also include policies and procedures to concerning the risk-based assessment of the customer relationship.[15]

(7) In accordance with chapter 3, section 1(2) of the AML Act, in assessing the money laundering and terrorist financing risks in a customer relationship, an obliged entity shall take into account the money laundering and terrorist financing risks relating to new and pre-existing customers, countries or geographic areas, as well as new, currently developed and already existing products, services, transactions, delivery channels and technologies (risk-based assessment).

(8) In accordance with chapter 3, section 1(4) of the AML Act, an obliged entity shall be able to demonstrate to the supervisory authority or a body appointed to supervise that their methods concerning customer due diligence and ongoing monitoring laid down in the AML Act are adequate in view of the risks of money laundering and terrorist financing.

(9) The FIN-FSA's authority to issue more detailed regulations on the procedures to be followed in customer due diligence and the management of risks posed by customers to the activities of a supervised entity is based on the following provisions: Section 39(4) of the Payment Institutions Act, chapter 15, section 18(4) of the Credit Institutions Act, section 13(4) of the Virtual Currency Providers Act, chapter 12, section 3(4) of the Investment Services Act, chapter 12, section 10 of the AIFM Act, chapter 6, section 21(4) of the Insurance Companies Act, chapter 26, section 15(4) of the Act on Common Funds and chapter 8, section 13 of the Act on the Book-Entry System and Settlement Operations.

(10) For the purposes of regulations 11–14, a supervised entity refers to supervised entities falling within the scope of authority to issue regulations under paragraph 9 above.

[15] *For more details on the risk-based assessment of the customer relationship, see chapter 5.3.*

REGULATION (paragraphs 11–14)

(11) Supervised entities shall have policies and principles based on a risk assessment referred to in chapter 2, section 3(1) of the AML Act to define the individual risk level of each customer, and the procedures shall reflect the provisions of chapter 3, section 1(2) of the AML Act on the factors to be taken into account in the risk-based assessment under chapter 3, section 1(2) of the AML Act.

(12) The procedures shall include processes to review the customer's risk level in order for the supervised entity to be able to adjust the customer due diligence procedures and monitoring of the customer relationship appropriately considering the customer's risk level, and where necessary, consider its risk appetite regarding the continuation of the customer relationship.

(13) Supervised entities shall determine the risk management methods applicable to the customer relationship based on the level of risk involved with the customer. In determining the risk management methods, supervised entities shall consider, in addition to the customer's risk level, also the factors on which the risk level is based.

(14) In determining a customer's risk level, supervised entities shall bear in mind that:

- The comprehensive determination of risk level is not necessarily affected by a single risk factor alone, unless the risk factor concerned requires the application of enhanced due diligence under a specific legal provision.
- The determination of the weights of the risk factors shall not be affected by the supervised entity's financial considerations or factors pertaining to the pursuit of operating profit.
- The procedure for the determination of the risk level shall not by nature unnecessarily lead to a situation where no customer relationship is classified as a high-risk one.
- The procedure for the determination of the risk level may not by nature unnecessarily lead to a situation where the majority of customer relationships are classified as lower-risk than normal.
- The determination of the customer's risk level may not contradict with the supervised entity's risk assessment.

GUIDELINE (paragraphs 15–16)

(15) The FIN-FSA recommends that the provisions of paragraphs 11–14 above are also complied with by supervised entities excluded from the authority to issue regulations under paragraph 9.

(16) The FIN-FSA recommends that, in applying the regulation in paragraph 13, supervised entities consider that a high-risk level stemming from different factors may require the application of different management methods.

6.3 Customer identification and identity verification

6.3.1 Definitions customer identification and identity verification

(17) In accordance with chapter 3, section 2(1) of the AML Act, obliged entities shall identify their customers and verify their identities when establishing a permanent customer relationship. In addition, obliged entities shall identify their customers and verify their identities in the case of:

1) a customer relationship of an irregular nature and:

a) the sum of a transaction or several linked operations amounting to EUR 15,000 or more;

b) transfer of funds in excess of EUR 1,000 referred to in Article 3(9) of the Payer Information Regulation; or

c) transaction in a service related to virtual currency as referred to in the Act on Virtual Currency Providers, the amount of which exceeds EUR 1,000;

2) the sum of a transaction in the sale of goods amounts to EUR 10,000 or more, whether the transaction is carried out in a single operation or in several operations which are linked, and the customer relationship is of an irregular nature;

3) a suspicious transaction or

4) the obliged entity has doubts about the reliability or adequacy of previously obtained verification data on the identity of the customer.

(18) In accordance with chapter 1, section 4(1)(6) of the AML Act, identification means establishing the customer's identity on the basis of information provided by the customer.

(19) In accordance with chapter 1, section 4(1)(7) of the AML Act, verification of identity means ascertaining the customer's identity on the basis of documents, data or information obtained from a reliable and independent source.

(20) In accordance with section Chapter 3, section 2(4) of the AML Act, obliged entities shall identify their customers and verify the identity of their customers when establishing a relationship with them or at the latest before their customers obtain control over the assets or other property involved in a transaction or before the transaction has been concluded.

GUIDELINE (paragraphs 21–27)

(21) According to the FIN-FSA's interpretation, the procedures referred to in chapter 2, section 3(2) of the AML Act shall include the supervised entity's risk-based procedures for customer identification and verification of identity both in establishing a customer relationship and other circumstances referred to in chapter 3, section 2(1) of the AML Act. The procedures shall indicate the sources considered reliable and independent within the meaning of chapter 1, section 4(7) of the AML Act by the supervised entity, and a report providing the justifications for such an assessment.

(22) The FIN-FSA recommends that, in assessing the reliability and independence of the sources referred to in chapter 1, section 4(7) of the AML Act, supervised entities consider paragraphs 4.26–4.28 of the EBA Risk Factors Guidelines.

(23) According to the FIN-FSA's interpretation, reliable and independent sources referred to in chapter 1, section 4(7) of the AML Act include at least registers maintained by the Finnish Patent and Registration Office (Trade Register, Register of Associations, Register of Foundations) and the population register maintained by the Digital and Population Data Services Agency.

(24) According to the FIN-FSA's interpretation, the monetary thresholds referred to in chapter 3, section 2 of the AML Act provide an absolute obligation to apply customer identification and

verification measures. However, for example a customer relationship involving several recurrent one-off transactions, may be justified to classify as a customer relationship even if the monetary thresholds provided in the law are not reached.

(25) The FIN-FSA recommends that supervised entities define in accordance with guideline 4.7 (b) of the EBA Risk Factors Guidelines what constitutes an occasional transaction in the context of their business and at what point a series of one-off transactions amounts to a business relationship, taking into consideration factors such as the frequency or regularity with which the customer returns for occasional transactions, and the extent to which the relationship is expected to have, or appears to have, an element of duration.

(26) According to the FIN-FSA's interpretation, the possibility referred to in chapter 3, section 2(4) of the AML Act not to conclude the verification of identity until after establishment of the customer relationship is an exception to the main rule, which shall be interpreted narrowly.

(27) According to the FIN-FSA's interpretation, chapter 3, section 2(4) of the AML Act means that the verification of identity can be concluded after the establishment of the customer relationship only where it is necessary to avoid the interruption of the customer's business and if the risk of money laundering and terrorist financing is low. Also in these circumstances, the customer identification and identity verification measures shall be concluded as fast as practically possible.[16]

6.3.2 Verification of the identity of a natural person

(28) The FIN-FSA's authority to issue more detailed regulations on the procedures to be followed in customer due diligence and the management of risks posed by customers to the activities of a supervised entity is based on the following provisions: Section 39(4) of the Payment Institutions Act, chapter 15, section 18(4) of the Credit Institutions Act, section 13(4) of the Virtual Currency Providers Act, chapter 12, section 3(4) of the Investment Services Act, chapter 12, section 10 of the AIFM Act, chapter 6, section 21(4) of the Insurance Companies Act, chapter 26, section 15(4) of the Act on Common Funds and chapter 8, section 13 of the Act on the Book-Entry System and Settlement Operations.

(29) For the purposes of regulation 35, a supervised entity refers to supervised entities falling within the scope of authority to issue regulations under paragraph 28 above.

GUIDELINE (paragraphs 30–34)

(30) According to the FIN-FSA's interpretation, a supervised entity may decide, relying on its risk-based procedures, what it documents and information it considers obtained from a reliable and independent source as referred to in chapter 1, section 4(7) of the AML Act, unless otherwise provided in other legislation.[17]

(31) The FIN-FSA also recommends that supervised entities consider the purpose for which the document was granted and in what process, when assessing what verification documents to consider reliable and independent within the meaning of chapter 1, section 4(7) of the AML Act. Based on a risk-based assessment, a supervised entity may create different procedures for the

[16] *Article 14 of 4AMLD.*
[17] *For example, section 17 of the Electronic Identification Act provides on the identification of a natural person applying for a means of identification. The Electronic Identification Act uses the term "proofing of a person's identity" as opposed to "verification" in the AML Act, both translated as verification into English. Chapter 7, section 15 of the Consumer Protection Act provides on the verification ("todentaminen") of the identity of a credit applicant.*

documentary evidence which shall be presented by customers to verify their identity on the one hand when establishing a customer relationship and on the other hand during the customer relationship.

(32) The FIN-FSA recommends that supervised entities create procedures for ascertaining the authenticity of a document used to verify identity.

(33) The FIN-FSA recommends that, when establishing their procedures for the verification of identity, supervised entities consider guidelines 4.9–4.11 of the EBA Risk Factors Guidelines when dealing with persons with legitimate and credible justifications for their inability to present conventional identity verification documents.

(34) The FIN-FSA recommends that, in circumstances referred to in paragraph 33, supervised entity assesses whether it is possible to provide only limited services to the customer and monitor the customer relationship on an enhanced basis to manage the risks pertaining to the customer relationship.

REGULATION (paragraph 35)

(35) In verifying one's identity with verification documents, supervised entities shall ascertain that the person resembles the person portrayed in the document in terms of appearance, age and other information presented in the document.

GUIDELINE (paragraph 36)

(36) The FIN-FSA recommends that regulation 35 is also complied with by supervised entities excluded from the authority to issue regulations under paragraph 28.

6.3.3 Verification of the identity of a legal person

(37) In accordance with chapter 1, section 4(7) of the AML Act, the verification of identity means ascertaining the customer's identity on the basis of documents, data or information obtained from a reliable and independent source.

(38) In accordance with chapter 3, section 2(3) of the AML Act, when another is acting on account of the customer (representative), the obliged entity shall also identify and verify the identity of the representative and ascertain the representative's right to act on behalf of the customer.

GUIDELINE (paragraphs 39–45)

(39) According to the FIN-FSA's interpretation, verification of identity under chapter 1, section 4(7) of the AML act means, as regards legal persons, that the existence of the legal person is verified with information and/or documents from a reliable and independent source.

(40) According to the FIN-FSA's interpretation, information from reliable and independent sources as referred to in chapter 1, section 4(7) of the AML Act include, as regards legal persons, among other things, information from public registers referred to in paragraph 23 above.

(41) The FIN-FSA recommends supervised entities to consider that not all countries have made available information in public registers which could be considered a reliable and independent

source within the meaning of chapter 1, section 4(7) of the AML Act. Supervised entities should carefully consider the up-to-datedness, reliability and usability from a foreign register (see chapter 6.3.1, paragraph 22 above).

(42) According to the FIN-FSA's interpretation, the obligation under chapter 3, section 2(3) of the AML act to identity a representative and verify the identity means, as regards legal persons, that the identity of the legal person's representative shall be verified similarly to a customer who is a natural person.[18]

(43) According to the FIN-FSA's interpretation, chapter 3, section 2(4) of the AML Act means that the identity of a legal person's representative shall, as a rule, be verified before starting a business relationship or executing a transaction, and the possibility to complete the verification of the identity of the legal person's representative only after the establishment of the customer relationship is an exception to the main rule.[19]

(44) According to the FIN-FSA's interpretation, the procedures referred to in chapter 2, section 3(2) of the AML Act shall include risk-based procedures to identify a legal person's representative, to verify the representative's identity and to ensure the right of representation.

(45) According to the FIN-FSA's interpretation, the representative's right to act on behalf of the customer may be ascertained in accordance with chapter 3, section 2(3) of the AML Act for example by checking the representative's right of signature on the excerpt from the Trade Register. The right of representation may also be based on, for example, the district court's decision to impose an administrator, or a power of attorney. Supervised entities shall assess the reliability of the document carrying the right of representation, and where necessary, take further steps to ascertain the right of representation.

6.3.4 Representative of a natural person

(46) In accordance with chapter 3, section 2(3) of the AML Act, when another is acting on account of the customer (representative), the obliged entity shall also identify and verify the identity of the representative and ascertain the representative's right to act on behalf of the customer.

(47) In accordance with section 4 of the Guardianship Services Act (442/1999), the custodians of a minor shall also be his/her guardians, unless otherwise provided elsewhere (see sections 24 and 25).

(48) As regards public guardians, chapter 3, section 3(2)(2) of the AML Act entering into force on 1 April 2023 specifically provides that the obliged entity shall retain, in lieu of the name, date of birth and personal identity code of the guardian, the service producer's identification information, title of the guardian and, where the service producer has more than one public guardian, the guardian's ordinal number.

GUIDELINE (paragraphs 49–56)

(49) According to the FIN-FSA's interpretation, representation referred to in chapter 3, section 2(3) of the AML Act may include, for example, the representation of a natural person by a power of

[18] *For more detailed information on the verification of the identity of a natural person, see chapter 6.3.2.*
[19] *For more detailed information, see chapter 6.3.2, paragraphs 26–27 above.*

attorney, the representation of a minor or the representation of a customer by a guardian assigned to the customer.

(50) According to the FIN-FSA's interpretation, the procedures referred to in chapter 2, section 3(2) of the AML Act should include risk-based procedures to identify the representative and to verify the representative's identity and right of representation.

(51) According to the FIN-FSA's interpretation, ascertaining the representative's right to act on behalf of the customer as referred to in chapter 3, section 2(3) of the AML Act means that the right of representation is verified based on a letter of authority, guardianship order or another document carrying the right of representation, or in another reliable manner. Supervised entities shall assess the reliability of the document carrying the right of representation, and where necessary, take further steps to ascertain the right of representation.

(52) According to the FIN-FSA's interpretation, the representative referred to in chapter 3, section 2(3) of the AML Act shall be identified and the identify verified in compliance with the provisions in chapter 6.3.2 above on the identification and verification of identity of a natural person.

(53) According to the FIN-FSA's interpretation, chapter 3, section 2(3) of the AML Act means that, when the custodians of a minor also function as his or her guardians, both custodians shall be identified and their identities verified in the context of establishing a customer relationship. Thereafter, the custodians may agree that one custodian is granted the authority to act on behalf of the minor before the other custodian's contribution.

(54) In accordance with the Government bill, the identification of a public guardian and verification of identity is possible indirectly based on information given by the service producer. Obliged entity should not copy a document used for identity verification or save the guardian's personal information as customer due diligence information, but obliged entity should only retain the information stated in the provision. However, the name and details of the postholder could be subsequently verified with the employer, if necessary, based on the information on the service producer and the ordinal number of the public guardian.[20]

(55) The FIN-FSA recommends that supervised entities pay particular attention to ensuring that the details of public guardians are not used in their systems so that they may be mixed with the information on the principals under guardianship, and that such circumstances do not arise where the safety and right to privacy of a public guardian would be compromised.

(56) The FIN-FSA also recommends that, in other circumstances than those referred to in paragraph 54 with respect to public guardianship, supervised entities ensure that the details of a guardian and a principal as a customer are not mixed in the supervised entities' systems.

6.3.5 Non-face-to-face identification

(57) If the customer is not physically present when he or she is identified and his or her identity verified (non-face-to-face identification), in accordance with chapter 3, section 11 of the AML Act, obliged entities shall take the following measures to reduce the risk of money laundering and terrorist financing:

[20] *Government Bill 236/2021, page 58-59.*

1) verify the customer's identity on the basis of additional documents, data or information obtained from a reliable source;

2) ensure that the payment relating to the transaction is made from a credit institution's account or into the account that was opened earlier in the customer's name; or

3) verify the customer's identity by means of an identification device referred to in the Act on Strong Electronic Identification and Electronic Signatures (617/2009) or a qualified certificate for electronic signature as provided in Article 28 of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC or other secure and verifiable electronic identification technology.

GUIDELINE (paragraphs 58–66)

(58) According to the FIN-FSA's interpretation, the risk assessment referred to in chapter 2, section 3 of the AML Act should consider risks related to non-face-to-face identification and related risk management measures, if the supervised entity uses non-face-to-face identification to customer identification and the verification of identity,

(59) In accordance with guideline 4.31 of the EBA Risk Factors Guidelines, the use of electronic means of identification does not of itself give rise to increased ML/TF risk, in particular where these electronic means provide a high level of assurance under Regulation (EU) 910/2014.[21]

(60) According to the FIN-FSA's interpretation, the procedures referred to in chapter 2, section 3(2) of the AML Act should include non-face-to-face procedures, if the supervised entity uses non-face-to-face identification in its activities. The procedures concerning non-face-to-face identification should indicate which sources the supervised entity considers reliable and independent within the meaning of chapter 1, section 4(1)(7) of the AML Act for the purposes of remote identity verification.

(61) According to the FIN-FSA's interpretation, chapter 3, section 11 of the AML Act means that customer identification and identity verification in the context of non-face-to-face identification may require the combination of several methods and requesting further information both from the customer and sources regarded as reliable and independent.

(62) According to the FIN-FSA's interpretation, the verification of identity in the context of non-face-to-face identification as referred to in chapter 3, section 11 of the AML Act shall be based on information and documents from reliable and independent sources referred to in chapter 4, section 1(7) of the AML Act.

(63) The FIN-FSA recommends that supervised entities applying remote identification in their activities, in connection with establishing a customer relationship, verify the customer's identity by means of an identification device referred to in the Act on Strong Electronic Identification and Electronic Signatures (617/2009) or a qualified certificate for electronic signature as provided in Article 28 of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC or other secure and verifiable electronic identification technology.

[21] *See also paragraph 2(c) of Annex III on higher-risk factors of 4AMLD.*

(64) The FIN-FSA recommends that supervised entities making use of non-face-to-face identification in their activities do not use the methods referred to in chapter 3, section 11(2) and (2) of the AML Act to verify the identity of a natural person in the context of establishing a customer relationship in a way that the verification of identity is only based on documentary evidence obtained from the customer and the fact that a payment related to a transaction comes from a credit institution's account or is paid to an account opened earlier in the customer's name.

(65) According to the FIN-FSA's interpretation, where the identity of a legal person is being verified in the context of establishing a customer relationship based on a non-face-to-face procedure, the supervised entity may observe chapter 3, section 11(1) of the AML Act, i.e. obtain additional documents, data or information obtained from a reliable source.

(66) The FIN-FSA recommends that, in verifying the identity of a representative of a natural person and a legal person, paragraph 63 be complied with.

Use of another electronic identification technology in identity verification

GUIDELINE (paragraphs 67–72)

(67) The FIN-FSA recommends that supervised entities take into consideration the guidance provided in paragraphs 4.32–4.37 of the EBA Risk Factors Guidelines on using innovative technological means to verify identity if they intend to adopt another electronic identification technology.

(68) The FIN-FSA recommends that supervised entities take into consideration the FATF Guidelines on Digital ID.

(69) The FIN-FSA recommends that supervised entities ensure the data security and verifiability of the method used. In this context, verifiability means the possibility to ascertain afterwards, which information was used for verification in each instance and when.

(70) The FIN-FSA recommends that, in considering the use of another electronic identification technology in the identification of a customer and the verification of identity, supervised entities assess the adequacy of the identification technology relative to the money laundering and terrorist financing risks involved.

(71) The FIN-FSA recommends that, in assessing the adequacy of an identification technology, supervised entities pay particular attention to ensuring that the verification of identity is made relying on documents or information from a reliable and independent source (on reliable sources, see chapter 6.3.1, paragraphs 22–23 above).

(72) According to the FIN-FSA's interpretation, a supervised entity shall ascertain that the customer due diligence information referred to in chapter 3, section 3 of the AML Act are available to it for fulfilling its obligations under the AML Act and that the information is retained in accordance with the law.

6.3.6 Special identification obligation relating to life and other investment-related insurance

(73) As regards life insurance and other investment-related insurance policies, chapter 3, section 5(1) of the AML Act provides on the obligation of credit and financial institutions to establish, in addition to the customer due diligence information under chapter 3 of the AML Act, the following:

1. the name of the beneficiary when a person is identified or named as the beneficiary;
2. in the case of beneficiaries classified by means other than those referred to in paragraph 1, sufficient information concerning those beneficiaries to enable the pay-out to take place when due.

(74) In accordance with chapter 3, section 5(2) of the AML Act, the identity of the beneficiary shall be verified at the time of the payout.

(75) In accordance with chapter 3, section 5(3) of the AML Act, when aware of the assignment, credit institutions and financial institutions shall identify at the time of assignment any third party to which or for the benefit of which a life insurance policy or investment-related policy is assigned.

(76) In accordance with chapter 3, section 5(4) of the AML Act, credit institutions and financial institutions shall ensure that they are in possession of sufficient information concerning the beneficial owners of a foreign trust or company service provider to enable their rights relating to the foreign trust or company services to be established.

(77) Chapter 3, section 5(5) of the AML Act, provides on the obligation to establish whether the beneficiary under the life insurance policy or other investment-related insurance policy is a politically exposed person by the time of the pay-out or the assignment of the policy in part or in full. If a higher than ordinary risk of money laundering and terrorist financing attaches to the insurance policy or its beneficiary, officials of the credit institution and financial institution shall additionally report the matter to the management of the facility before pay-out and comply with the provisions concerning enhanced customer due diligence.

GUIDELINE (paragraphs 78–83)

(78) According to the FIN-FSA's interpretation, chapter 3, section 5 of the AML Act means that a supervised entity that provides life and other investment-related insurance policies shall ensure that it will obtain information on the beneficiaries of life insurance policies and other investment-related policies as soon as the beneficiaries have been specified or named.

(79) The FIN-FSA recommends that if beneficiaries have been specified using their name, the supervised entity should also record their personal identity number, date of birth or another corresponding identifier.

(80) According to the FIN-FSA's interpretation, chapter 3, section 5(1)(2) of the AML Act entails that where beneficiaries are not named but specified instead for example by the characteristics of a group, the supervised entity should obtain adequate information on these beneficiaries in order to ascertain that it is able to verify the identity of the beneficiary at the time of paying a claim.

(81) According to the FIN-FSA's interpretation, chapter 3, section 5(2) of the AML Act entails that the identity of a beneficiary is verified at the time of paying a claim in compliance with the provisions of the verification of the customer's identity. Guidelines on the verification of the identity of a natural person are provided in chapter 6.3.2 and on non-face-to-face identification in chapter 6.3.5. There are guidelines on the verification of a legal person's identity in chapter 6.3.3.

(82) According to the FIN-FSA's interpretation, the obligation under chapter 3, section 5(3) of the AML Act to identify third parties to whom a life or investment-related insurance policy is transferred applies to circumstances where a payment instruction concerning an insurance product is

assigned partly or completely to a third party. Subsequently, when a credit and financial institution becomes aware of the payment order, it shall identify the payee regardless of whether it is a natural person, a legal person or another ownership arrangement, such as a trust.

(83) According to the FIN-FSA's interpretation, in conducting the risk-based assessment referred to in chapter 3, section 1(2) of the AML Act, the supervised entity shall also consider the risks related the beneficiary of the insurance policy and take measures commensurate with the risks involved in the customer relationship. If the risk is elevated, the supervised entity shall assess the need for enhanced identification measures.

6.4 Customer due diligence information

6.4.1 Collection of customer information

(84) Chapter 3, section 3(2) of the AML Act provides on the customer due diligence information to be retained. Paragraphs 1–7 of the subsection provide on the retention of such basic information as the customer's name and address.

(85) In accordance with chapter 3, section 3(2)(8) of the AML Act, information on the customer's activities, nature and extent of business, financial standing, grounds for use of transaction or service and information on source of funds as well as the other necessary information referred to in section 4(1) acquired for the purpose of customer due diligence.

(86) In accordance with chapter 3, section 4(1) of the AML Act, obliged entities shall obtain information on their customers' and their beneficial owners' activities, the nature and extent of their business, and the grounds for the use of the service or product. Obliged entities may use available data from different information sources on the customer or its beneficial owner for the purpose of preparing and maintaining a risk assessment of the customer, preventing money laundering and terrorist financing and meeting the reporting obligation and the obligation to obtain information referred to in said Act.

(87) Furthermore, chapter 3, section 4(1) of the AML Act provides that obliged entities shall pay special attention to the credibility and reliability of the information source.

(88) In accordance with chapter 3, section 3(2)(9) of the AML Act, the information to be retained also include the necessary information acquired in order to fulfil the obligation to obtain information under section 4(3).[22]

GUIDELINE (paragraphs 89–98)

(89) According to the FIN-FSA's interpretation, the purpose of the obligation to obtain customer due diligence information under chapter 3, section 4 of the AML Act is to ensure that supervised entities have adequate information to assess the risks involved in a customer relationship and to determine the individual risk level of the customer.[23]

(90) According to the FIN-FSA's interpretation, supervised entities shall define the information under chapter 3, section 3(2)(8) of the AML Act applying a risk-based approach it considers necessary to determine the customer's risk level with a view to risk factors related to different products and

[22] *On the obligation to obtain information, see chapter 7.2.*
[23] *On the risk-based assessment of the customer relationship, see chapter 6.2, in particular regulations 11–14.*

services as well as customer groups. The extent of customer due diligence information obtained by supervised entities for customer due diligence purposes may vary on a risk-sensitive basis. In addition, the risk management measures applied by the supervised entity has an impact on how extensively information shall be collected on the customer.

(91) According to the FIN-FSA's interpretation, chapter 3, section 4(1) of the AML Act means that supervised entities shall determine, applying a risk-based approach, from which sources and how to collect information for customer due diligence purposes when establishing the customer relationship and during the customer relationship. The sources may include various official sources and other reliable and independent sources, but some of the information may be collected directly from the customer.

(92) According to the FIN-FSA's interpretation, a supervised entity shall resolve applying a risk-based approach what information sources it considers credible and reliable as referred to in chapter 3, section 4(1) of the AML Act, and it shall also assess the degree of reliability of information obtained from the source. In order to ascertain the credibility and reliability of information, it may be necessary for the supervised entity to examine the accuracy of information from several information sources considered reliable by it.

(93) The Government bill[24] describes in more detail the various sources of available information on the customer or its beneficial owner which can be utilised by obliged entities in order to comply with the customer due diligence obligation. The information sources may include for example court decisions, information reported in the media and information from official registers. However, obliged entities shall pay special attention to the credibility and reliability of the information source. If a piece of information is based on information presented in the public domain, the obliged entity should consider it with particular caution, since it does not usually have an effective possibility to assess the reliability of the source that presented the information. For example, caution should be applied to entering information in the customer register solely based on media reports.

(94) According to the FIN-FSA's interpretation, obtaining information on the grounds for the use of the service or product as referred to in chapter 3, section 4(1) of the AML Act means that the supervised entity shall review why the customer wants to enter a customer relationship with it, and which of the supervised entity's products and services, and how, the customer intends to use.

(95) The FIN-FSA recommends that supervised entities comply with the minimum measures listed in paragraph 4.38 of the EBA Risk Factors Guidelines to examine the nature and purpose of the customer relationship.

(96) According to the FIN-FSA's interpretation, where a supervised entity provides basic banking services referred to in chapter 15, section 6 of the Credit Institutions Act and, according to the supervised entity's risk assessment, the customer relationship does not involve higher than ordinary risk of money laundering and terrorist financing, at least the following information shall be reviewed and retained in the context of establishing and maintaining a customer relationship:

- information referred to in chapter 3, section 3(2), paragraphs 1, 2 and 7 of the AML Act

[24] *Government bill 38/2018, p. 22.*

- whether the customer or the customer's beneficial owner is or has been a politically exposed person, a family member of a politically exposed person or a person known to be an associate of a politically exposed person as referred to in chapter 3, section 13 of the AML Act
- under chapter 3, section 3(2)(8) of the AML Act
  - information on the customer's situation of life as regards financial position (for example wage earner, retiree, student)
  - indication of whether the relationship is the customer's primary banking relationship
  - information on the origin or source of the funds and regular payment transactions / money flows
  - estimate of the customer's regular payment volume
  - estimate of the customer's foreign payments and grounds of these payments

(97) According to the FIN-FSA's interpretation, the address as referred to in chapter 3, section 3(2)(1) of the AML Act refers as a rule to the address of the customer's permanent place of residence.

(98) According to the FIN-FSA's interpretation, as regards the address of domicile referred to in chapter 3, section 3(2)(1) of the AML Act, it is enough as a rule that the supervised entity records the customer's contact address through which the customer can be reached by letter mail if the customer does not have a permanent or temporary address, or the customer does not want to disclose the address due to a valid non-disclosure for personal safety. The supervised entity shall assess on a risk-sensitive basis the importance of the lack of the customer's home address on the overall risk involved in the customer relationship and whether the supervised entity is able to manage these risks. The management of risks related to the customer relationship may require for example enhanced monitoring or other enhanced customer due diligence measures.

6.4.2 Processing of information on criminal convictions and offences

(99) In accordance with chapter 3, section 3 a(1) of the AML Act, obliged entities have the right to use and otherwise process as customer due diligence information such information concerning a criminal sentence or criminal act pertaining to the customer or its beneficial owner that is publicly available and necessary for:

1. the assessment of money laundering/terrorist financing risk related to the customer relationship; or
2. the performance of the obligation to obtain information pertaining to an unusual transaction in accordance with chapter 3, section 4 of the AML Act.

(100) In accordance with chapter 3, section 3 a (2) of the AML Act, the personal data referred to in chapter 3, section 3 a (1) of the AML Act must be related to money laundering, terrorist financing or such crimes as were committed to gain the assets or proceeds of crime subject to money laundering or terrorist financing.

(101) In accordance with chapter 3, section 3 a (3) of the AML Act, obliged entities have the right to process personal data referred to in chapter 3, section 3 a (1) of the AML Act, where it is derived from a reliable source, accurate and up-to-date.

(102) In accordance with chapter 3, section 3 a (4) of the AML Act, obliged entities have the right to process personal data referred to in chapter 3, section 3 a (1) of the AML Act, where they have procedures in place allowing them to differentiate between a criminal charge, investigation, trial and conviction, with a view to the basic right to have a fair trial, the right to defend oneself and the presumption of innocence.

(103) In accordance with chapter 3, section 3 a (5) of the AML Act, personal data referred to in chapter 3, section 3 a (1) of the AML Act must be retained separately from the customer register and removed at the latest in five years from the date when the data was first registered.

(104) In accordance with chapter 3, section 3 a(6) of the AML Act, the provisions of section 6(2) of the Data Protection Act on the safeguarding of the rights of the data subject also apply to personal data referred to in subsection 1 of the abovementioned section.

GUIDELINE (paragraphs 105–107)

(105) Paragraph 2.5 of EBA Risk Factors Guidelines presents risk factors that may be relevant when identifying the risk associated with the reputation of a customer or a customer's beneficial owner.

(106) According to the Government bill[25] the processing of data referred to in chapter 3, section 3 a (1) of the AML Act would always require the obliged entity to consider whether the requirement of necessity is met. The provision would give obliged entities the right to process sensitive personal data in necessary circumstances in order to be able to appropriately assess and manage risks to prevent money laundering and terrorist financing. As a source, obliged entities could use generally available information, such as so-called adverse media information, indicating criminal suspicions or convictions. Adverse media information refers to negative information on the customer derived from different media sources.

(107) According to the Government bill,[26] the specific requirement of a protection measure under chapter 3, section 3 a (5) of the ALM Act requires that the information must be retained separately from the customer register. This would ensure that the information is only processed by those who have a specific need pertaining to their duties. The data subjects would have the right of access to the data in accordance with Article 14 of the General Data Protection Regulation. The data subjects would also have the right to obtain the rectification of data concerning as provided in Article 16 of the General Data Protection Regulation.

6.4.3 Identification of the beneficial owner

(108) In accordance with chapter 3, section 6(1), obliged entities shall identify and maintain adequate, precise and up-to-date information about the customers' beneficial owners and, when necessary, verify their identity.

(109) A beneficial owner is defined in chapter 1, section 5 of the AML Act.

(110) In accordance with chapter 1, section 5 of the AML Act, the beneficial owner of a corporation refers to a natural person who ultimately:

[25] *Government Bill 236/2021 p. 59.*
[26] *Government Bill 236/2021 p. 60.*

1. directly or indirectly owns more than 25% of the shares in a legal person or otherwise has an equivalent ownership interest in the legal person;
2. directly or indirectly exercises more than 25% of the votes in a legal person and these votes are based on ownership, membership, articles of association, partnership agreement or equivalent instrument; or
3. in any other way effectively exercises control of a legal person.

(111) In accordance with chapter 1, section 5(2) of the AML Act, an ownership interest of more than 25% in the relevant legal person held by a natural person is an indication of direct ownership.

(112) In accordance with chapter 1, section 5(3) of the AML, the following is an indication of indirect ownership:

1. a legal person in which one or more natural persons exercise independent control holds an ownership interest of more than 25% in the relevant legal person or more than 25% of the votes in the relevant legal person; or
2. a natural person or a legal person in which the natural person exercises independent control has the right, based on ownership, membership, articles of association, partnership agreement or equivalent instrument, to appoint or dismiss the majority of the members of the board of directors or equivalent body of the relevant legal person.

(113) In accordance with chapter 1, section 5(4) of the AML Act, if the beneficial owner cannot be identified or if the conditions laid down in subsection 1 are not met, the relevant legal person's board of directors or active partners, managing director or another person holding an equivalent position are to be considered the beneficial owners.

(114) In accordance with chapter 3, section 6(2) of the AML Act, obliged entities shall keep a record of the identification measures concerning the beneficial owner.

(115) In accordance with chapter 3, section 1(1) of the AML Act, if an obliged entity is unable to carry out the customer due diligence measures laid down in chapter 3 of the AML Act, the entity may not establish a customer relationship, conclude a transaction or maintain a business relationship

GUIDELINE (paragraphs 116–130)

(116) According to the Government bill,[27] the position of the beneficiary in circumstances referred to in chapter 1, section 5(1)(1–2) of the AML Act is based on facts that can be verified for example by reference to the shareholder register or the legal person's rules.

(117) In accordance with the Government bill,[28] the obliged entity shall also examine, in an effective and appropriate way concerning the ML/TF risks related to the customer, whether there is a third party exercises control as referred to in chapter 1, section 5(1)(3) in the customer. For example, such control may be based on a partnership agreement or the exercise of control through ownership interests lower than 25 percent. In such circumstances, it may not always be possible to find out the beneficial owner; therefore the obliged entity should determine customer

[27] *Government bill 228/2016, p.106.*
[28] *Government bill 228/2016, p. 106.*

identification measures appropriate with a view to the money laundering risks related to the customer.

(118) According to the FIN-FSA's interpretation, the possibility under chapter 1, section 5(4) of the AML Act to consider the relevant legal person's board of directors or active partners, managing director or another person holding an equivalent position the beneficial owners is an exception which should be applied only if the supervised entity is unable to determine in a manner appropriate to the risks of money laundering and terrorist financing relating to the customer and to an adequate extent the beneficial owner whose position is based on ownership or control.[29]

(119) According to the FIN-FSA's interpretation, supervised entities may apply chapter 1, section 5(4) of the AML Act for example when ownership is so fragmented that each holder's share of ownership and votes fall below 25% and no other party effectively exercises control within the meaning of chapter 1, section 5(1)(3) of the AML Act in the legal person.

(120) According to the FIN-FSA's interpretation, the exception provided in chapter 1, section 5(4) of the AML Act cannot be applied in circumstances where a customer refuses to disclose information on beneficial owners, but it only applies to circumstances where a beneficial owner cannot be identified based on ownership or control.

(121) According to the Government bill,[30] obliged entities may utilise registers concerning beneficial owners in meeting their customer due diligence and identification obligations. However, obliged entities may not solely rely on this information in meeting their customer due diligence and identification obligations concerning beneficial owners.

(122) The FIN-FSA recommends supervised entities to consider that the usability of registered information may be limited for example by circumstances where information on beneficial owners has not been updated or the supervised entity has grounds to suspect their accuracy.

(123) In accordance with the Government bill,[31] measures to be taken to identify beneficial owners that should be recorded by the obliged entity in accordance with chapter 3, section 6(2) of the AML Act include, for example, how often the information on beneficial owners have been checked and updated, where they have been checked, for example the customer, a public register or other public source, and how the information has been evaluated for example in terms of reliability, and any further reviews that have been undertaken.

(124) According to the FIN-FSA's interpretation, where a supervised entity has assessed that the customer relationship involves a low risk of money laundering and terrorist financing, it is adequate and appropriate within the meaning of chapter 3, section 6(1) of the AML Act to obtain a report on beneficial owners from the customer and compare this information to the information in registers referred to in chapter 6 of the AML Act.

(125) According to the FIN-FSA's interpretation, where a supervised entity has assessed that the customer relationship involves an elevated risk of money laundering and terrorist financing, the requirement of adequate and appropriate information of chapter 3, section 6(1) of the AML Act requires more extensive documented evidence about the identity of the beneficial owner. This may mean, for example, the utilisation of external service providers and establishing the owners

[29] *For more detail, see also Article 3(6a)(ii) of 4AMLD.*
[30] *Government bill 228/2016, p. 106.*
[31] *Government bill 261/2020, p. 21.*

of group companies based on documentary evidence and an extract from the Trade Registry and articles of association of these companies.

(126) According to the FIN-FSA's interpretation, in circumstances referred to in paragraph 124, where complex ownership structures are concerned, the supervised entity should, so as to comply with the requirement of chapter 3, section 6(1) of the AML Act on maintaining information, find out the customer's group structure so that the report indicates the chain of ownership or voting power from the customer to each beneficial owner.

(127) According to the FIN-FSA's interpretation, by virtue of chapter 3, section 6(1) of the AML and chapter 3, section 3(1) of the AML Act, a supervised entity shall check the information on beneficial owners and update them where necessary when it becomes aware of significant changes pertaining to the customer. For example, information on beneficial owners shall be updated in the context of a business sale, merger and demerger.

(128) According to the FIN-FSA's interpretation, if a supervised entity, in conducting risk-based assessment under chapter 3, section 3(1) of the AML Act, considers that there is increased risk of money laundering and terrorist financing associated with the customer, it shall assess whether its information on beneficial owners is adequate or whether it should take enhanced due diligence actions.

(129) According to the FIN-FSA's interpretation, supervised entities shall, applying risk-based assessment, decide when the identification of the beneficial owner is necessary within the meaning of chapter 3, section 6(1) of the AML Act.

(130) According to the FIN-FSA's interpretation, where a supervised entity has considered the identification of the beneficial owner necessary within the meaning of chapter 3, section 6(1) of the AML Act, the identity of the beneficial owner shall be verified in accordance with chapter 3, section 2(4) of the AML Act before entering into a business relationship or executing a transaction. The verification of identity can be concluded after the commencement of the business relationship where necessary to avoid the interruption of business and where the ML&TF risk is low.

Reporting obligation to the Patent and Registration Office

(131) In accordance with chapter 6, section 5 of the AML Act, where an obliged entity observes any deficiency or inconsistency in its customers' registered information in the Trade Register, register of associations, register of religious communities and register of foundations, it shall without undue delay notify this to the party maintaining the register[32] (*discrepancy report*)[33].

GUIDELINE (paragraphs 132–139)

(132) According to the FIN-FSA's interpretation, chapter 6, section 5 of the AML Act enables a supervised entity to request a customer to update its information on the beneficial owners if the supervised entity identifies deficiencies or inconsistencies therein.

[32] *In Finland, the Trade Register, register of associations, register of religious communities and register of foundations are maintained by the Patent and Registration Office.*
[33] *Instructions on filing a discrepancy report are published on the website of the Patent and Registration Office.*

(133) According to the FIN-FSA's interpretation, no undue delay as referred to in chapter 6, section 5 of the AML Act arises if the supervised entity reserves about a week for updating the information before filing a discrepancy report.

(134) According to the FIN-FSA's interpretation, no discrepancy report referred to in chapter 6, section 5 of the AML Act has to be made if the customer updates the information on its beneficial owners in the register within the deadline referred to in paragraph 133.

(135) According to the FIN-FSA's interpretation, no discrepancy report referred to in chapter 6, section 5 of the AML Act has to be made if information on the customer's beneficial owners has not been entered in the register at all.

(136) According to the FIN-FSA's interpretation, filing a discrepancy report referred to in chapter 6, section 5 of the AML Act does not affect the responsibility of the supervised entity to identify its beneficial owners in accordance with chapter 3, section 6 of the AML Act.

(137) The FIN-FSA recommends a supervised entity recommends its customer to file a notification of its beneficial owners without delay if the customer's beneficial owners have not been entered in the register at all.

(138) The FIN-FSA recommends that the supervised entity assesses in its customer-specific risk assessment the customer's significance for total risk if the customer has not notified information its beneficial owners for registration or kept it up to date.

(139) The FIN-FSA recommends that if a customer fails to take actions to enter accurate and up-to-date information on beneficial owners in the register, the supervised entity assesses whether there are grounds to file suspicious transaction report.

6.4.4 Retention and updating of customer due diligence data

(140) In accordance with chapter 3, section 3(1) of the AML Act, obliged entities shall ensure that all documents and data concerning customer due diligence and customer transactions are up to date and relevant. The data shall be retained in a reliable manner for a period of five years after the end of the permanent customer relationship. In the case of occasional transactions referred to in section 2, subsection 1, paragraphs 1 and 2 or in subsection 2 of the said section, customer due diligence data shall be retained for a period of five years from the conclusion of the transaction.

(141) Chapter 3, section 3(2) determines in more detail which customer due diligence information shall be retained at the minimum.

(142) In accordance with chapter 3, section 1(3) of the AML Act, the customer due diligence measures laid down in chapter 3 of the AML Act shall be observed throughout the course of the customer relationship on the basis of risk-based assessment.

(143) In accordance with chapter 3, section 2(1)(4) of the AML Act, obliged entities shall identify their customers and verify their identities if they have doubts about the reliability or adequacy of previously obtained verification data on the identity of the customer.

(144) In accordance with chapter 7, section 2(1) of the AML Act, notwithstanding secrecy obligations, obliged entities shall without undue delay and free of charge supply the supervisory authorities

with the information and reports requested by it to enable the performance of the duties referred to in said Act or in provisions issued under it.

GUIDELINE (paragraphs 145–152)

(145) According to the FIN-FSA's interpretation, to fulfil the authority's right to obtain information under chapter 7, section 2(1) of the AML Act, a supervised entity shall arrange the retention of documents and data referred to in chapter 3, section 3 of the AML Act so that it is able to provide the data to the FIN-FSA without undue delay.

(146) According to the FIN-FSA's interpretation, the obligation referred to in chapter 3, section 3(1) of the AML Act to keep data concerning customer due diligence up to date and relevant and the obligation to retain this data mean that supervised entities shall keep a complete and solid audit trail across customer due diligence data collected at different points in time.

(147) According to the FIN-FSA's interpretation, the supervised entity shall, as part of the procedures referred to in chapter 2, section 3(2) define procedures to ensure the accuracy, up-to-datedness and relevance of the data. This means, for example, the definition of regular updating cycles for different customer groups based on their risk level so that if a customer or business relationship is assessed to involve a higher than ordinary risk of money laundering or terrorist financing, the up-to-datedness, reliability and relevance of the customer due diligence data shall be assessed more frequently.

(148) According to the FIN-FSA's interpretation, the requirement of the up-to-datedness and relevance of information in chapter 3, section 3(1) applies to information which is necessary to know the customer due to the application of a risk-based approach.

(149) According to the FIN-FSA's interpretation, the requirement of the up-to-datedness and relevance of customer due diligence data provided in chapter 3, section 3(1) means that, in updating customer due diligence data, observations made in ongoing monitoring referred to in chapter 3, section 4(2) of the AML Act and other information accrued by the supervised entity on the customer during the customer relationship shall be taken into account.

(150) In accordance with the Government bill,[34] if the document used to verify the customer's identity has expired during the customer relationship and the customer uses strong electronic identification, the requirement of the up-to-datedness and relevance of information does not necessitate requiring the customer to present a new identification document to continue the customer relationship.

(151) According to the FIN-FSA's interpretation, the requirement of the up-to-datedness and relevance of information provided in chapter 3, section 3(1) of the AML Act does not require that the customer's identity is verified again every time the identification document expires, since identity as a rule is not an information item that expires.

Example:

Where the supervised entity is able to automatically check in the Population Information System the up-to-datedness of the identification information of a person with a Finnish personal ID, re-verification of identity is not necessarily required.

[34] *Government bill 38/2018, p. 22.*

(152) According to the FIN-FSA's interpretation, the re-verification of identity may be necessary, in addition to circumstances referred to in chapter 3, section 2(1)(4) of the AML Act, where the verification of information on the basis of reliable sources is not feasible, for example regarding foreign customers.

6.5 Simplified customer due diligence obligation

6.5.1 Simplified customer due diligence procedure

(153) In accordance with chapter 3, section 8 of the AML Act, in applying chapter 3, sections 2–4 and 6 of the AML Act, obliged entities may observe a simplified customer due diligence procedure when, based on the risk assessment, they assess the risk of money laundering and terrorist financing associated with the customer relationship or transaction to be negligible in nature. However, obliged entities shall monitor customer relationships in the manner referred to in section 4, subsection 2 of this chapter in order to detect any unusual or suspicious transactions

(154) In accordance with section 1(2) of Government Decree 929/2021, when adjusting the measures included in the simplified customer due diligence procedure referred to in chapter 3, section 8 of the AML Act, obliged entities shall ensure that the customer due diligence measures are adequate relative to the risks involved in the service, new and existing product or transaction, distribution channel, technology, geographical area or customer relationship and in order to detect any exceptional or unusual transactions.

GUIDELINE (paragraphs 155–162)

(155) According to the FIN-FSA's interpretation, the simplified procedure under chapter 3, section 8 of the AML Act does not allow supervised entities not to comply with one or more of the requirements provided in chapter 3, sections 2–4 and 6 of the AML Act concerning customer due diligence. The simplified procedure enables the adjustment of customer due diligence procedures and one, several, or all individual customer due diligence actions and ongoing customer monitoring actions. Hence, all obligations under chapter 3, sections 2–4 and 6 of the AML Act shall be fulfilled, but they may be fulfilled following a lighter procedure.

(156) According to the FIN-FSA's interpretation, chapter 3, section 8(1) of the AML Act does not require supervised entities to apply simplified customer due diligence in circumstances involving a low ML/TF risk.

(157) According to the FIN-FSA's interpretation, if a supervised entity intends to apply a simplified procedure referred to in chapter 8, section 8(1) of the AML Act, the supervised entity shall, as part of the procedures referred to in chapter 2, section 3(2) of the AML Act prepare procedures for complying with the simplified customer due diligence obligation. The simplified procedure does not have to be similar in all low-risk circumstances.

(158) According to the FIN-FSA's interpretation, compliance with the simplified customer due diligence procedure as referred to in chapter 3, section 8 of the AML Act requires that the supervised entity has specifically assessed whether the customer or individual transaction involves such risk factor due to which the customer or transaction should not be classified as low-risk. In order that the supervised entity could make this assessment, it shall obtain adequate information on the customer and the nature and extent of its business. The assessment shall not be based on any

single risk factor, but the customer relationship and the risk factors involved shall be considered as a whole.

(159) According to the FIN-FSA's interpretation, based on chapter 3, section 8 of the AML Act, customers can be grouped so that a group of customers involving low risk is subject to a similar customer due diligence procedure. However, the application of a simplified customer due diligence procedure requires that there are no such considerations that would elevate the ML/TF risk related to an individual customer relationship in a way that, when assessed as a whole, the risk associated with the customer relationship could no longer be considered low.

For example, this kind of customer groups which could be subject to a simplified customer due diligence procedure if the customer relationship does not involve special risk-elevating considerations, include:

- a limited liability housing company whose primary purpose is to own and control apartments possessed by the shareholders
- a private road maintenance association only engages in private road maintenance activities
- a joint ownership association managing a common water area only engaging in water area management and activities customarily related to fishing in it
- a ditch drainage corporation established by landowners, only engaged activities related to the execution of joint ditch drainage and maintenance

(160) The FIN-FSA recommends that supervised entities reflect on the following questions in assessing whether the housing company customers referred to above in paragraph 159 involve any special characteristics that would elevate the associated ML/TF risk:

- Does the housing company use the supervised entity's products and services in a manner typical of housing companies?
- Does the housing company pursue leasing of commercial premises to a significant extent, and if it does, do the tenants involve risk-elevating characteristics for example due to operating in fields typically associated with higher money laundering risk (for example a company whose business involves many large cash payments)?
- Is the supervised entity aware that there is an elevated money laundering risk related to a member of the board of the housing company or an owner holding a significant proportion of the housing company's shares?

(161) According to the FIN-FSA's interpretation, the application of a simplified due diligence procedure as refer to in chapter 3, section 8 of the AML Act does not free the supervised entity from carrying out ongoing monitoring in accordance with chapter 3, section 4(2) of the AML Act. The supervised entity shall observe and pay attention to such changes in the customer's circumstances or activities, based on which the customer can no longer be considered a low-risk customer and thereby within the scope of the simplified customer due diligence procedure.

(162) The FIN-FSA recommends that, in preparing simplified customer due diligence procedures, supervised entities take into account the following possibilities to ease the customer due diligence procedure:

- The supervised entity carries out the customer due diligence procedures to update customer due diligence information less frequently in comparison with normal or above-normal-risk customers.

- The supervised entity does not specifically obtain information on the purpose of the customer relationship, since this can be deduced based on the type of product or service used by the customer, where the product or service concerned has been designed for a single purpose and the product or service type does not involve high risk in itself.
- The supervised entity carries out ongoing monitoring of the customer and customer relationship on a more limited scale than with higher-risk customers, for example adjusting the frequency and intensity of ongoing monitoring. Ongoing monitoring may also be adjusted by only monitoring transactions above a certain threshold. However, when applying a threshold, the supervised entity shall ensure that the threshold is set at a reasonable level and the system is able to identify linked transactions whose combined value would exceed the threshold.

6.6 Enhanced customer due diligence obligation

6.6.1 Enhanced customer due diligence procedure

(163) In accordance with chapter 3, section 10 of the AML Act, an obliged entity shall apply the enhanced customer due diligence procedure

1) in cases referred to in sections 11-13 and 13 a of the AML Act
2) if, based on the risk assessment, it estimates a higher than ordinary risk of money laundering and terrorist financing to attach to the case; or
3) if the customer or the transaction is linked to a state whose system for preventing and investigating money laundering and terrorist financing, in the European Commission's estimation, constitutes a significant risk to the internal market of the European Union or does not meet international obligations.

(164) Chapter 3, sections 11–13 a of the AML Act provides on enhanced procedures pertaining to non-face-to-face identification, correspondent banking relationships, politically exposed persons and high-risk non-EEA member states (high risk third countries). The procedures applicable in these circumstances are described in more detail in the Act, which leaves less room for discretion to the supervised entity than when only applying chapter 3, section 10 of the AML Act.

(165) Government decree 929/2021 provides on the simplified and enhanced customer due diligence procedure as well as low or higher-than-normal risk factors pertaining to the prevention and examination of money laundering and terrorist financing.

GUIDELINE (paragraphs 166–171)

(166) According to the FIN-FSA's interpretation, as part of the procedures referred to in chapter 2, section 3(2) of the AML Act, supervised entities shall prepare enhanced customer due diligence procedures for circumstances referred to in chapter 3, section 10 of the AML Act.

(167) According to the FIN-FSA's interpretation, the enhanced customer due diligence procedure provided in chapter 3, section 10 of the AML Act complements the normal customer due diligence procedure in circumstances where the case is considered to involve a higher-than-normal risk of money laundering and terrorist financing. The enhanced procedure seeks to manage risks more effectively in circumstances involving higher risk than normal.

(168) According to the FIN-FSA's interpretation, supervised entities may prepare several procedures to comply with the enhanced customer due diligence requirement under chapter 3, section 10 of the AML Act depending on the factors underlying the higher risk.

(169) According to the FIN-FSA's interpretation, the obligation to apply the enhanced customer due diligence procedure under chapter 3, section 10 of the AML Act may arise when establishing a customer relationship or during the relationship.

(170) The FIN-FSA recommends that, when preparing their own customer due diligence procedures, supervised entities consider the examples presented in the EBA Risk Factors Guidelines on situations involving higher-than-normal risk and actions to be taken to comply with the enhanced customer due diligence obligation. The enhanced procedure may include, for example, the following measures:

- obtaining information from the customer's place of birth
- obtaining more detailed information from sources other than the customer
- obtaining additional information on the customer, such as the purpose and intended nature of the customer relationship
- obtaining information on the customer's wealth and the source of funds
- verifying identity on the basis of reliable and independent sources
- carrying out the customer due diligence more frequently than normal throughout the customer relationship
- conducting a regular review of the customer's transactions
- obtaining more detailed information on the customer's business
- obtaining additional information on the customer's beneficial owners and beneficiaries
- examining the customer's previous business activities
- researching the customer and its beneficial owners for example through an online search
- obtaining senior management's approval for the establishment or continuation of the customer relationship

(171) According to the FIN-FSA's interpretation, chapter 3, section 10(1) of the AML Act does not mean that higher-than-normal risk associated with a customer relationship or individual transaction would automatically prevent the supervised entity from entering into the customer relationship or executing the transaction. In these circumstances, the supervised entity is obliged to apply enhanced customer due diligence in order to manage the higher-than-normal ML/TF risks.

6.6.2 Enhanced customer due diligence obligation related to politically exposed persons

(172) A politically exposed person (PEP), members of the family of a politically exposed person and close associate of a politically exposed person are defined in chapter 1, section 4(1)(11)– (13) of the AML Act.

(173) In accordance with chapter 3, section 13(1) of the AML Act, obliged entities shall have in place appropriate risk-based procedures to determine whether the customer is or has been a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person.

(174) In accordance with chapter 3, section 13(2) of the AML Act, political exposure shall be determined whenever the obliged entity based on the obliged entity's risk assessment referred to in chapter 2, subsection 3 assesses that a higher than ordinary risk of money laundering or terrorist financing attaches to the customer relationship or an individual transaction.

(175) In accordance with the transitional provisions concerning chapter 3, section 13(3) of the AML Act entering into force on 1 April 2023, where the customer or the customer's beneficial owner is a politically exposed person or a family member of such a person, or a person known to be an associate of such a person:

1) the senior management of the obliged entity shall give its approval for establishment of a customer relationship with the person;

2) the obliged entity shall take appropriate steps to determine the source of the assets and funds relating to the said customer relationship or transaction; and

3) the obliged entity shall put in place enhanced ongoing monitoring of the customer relationship.

(176) Until 31 March 2023, the measures referred to above in paragraph 175 shall also apply to circumstances where the customer or the customer's beneficial owner is a politically exposed person or a family member of such a person, or a person known to be an associate of such a person.[35]

(177) In accordance with chapter 3, section 13(4) of the AML Act, where a person is no longer entrusted with a prominent public function, obliged entities shall, for at least 12 months, be required to take into account the continuing risk posed by that person and to apply appropriate and risk-sensitive measures until such time as that person is deemed to pose no further risk specific to politically exposed persons.

(178) Until 31 March 2023, in accordance with chapter 3, section 13(4) of the AML Act, a person is no longer considered a politically exposed person when he or she has not held an important public position for at least one year

(179) The Government Decree on Important Public Positions within the Meaning of the Act on the Prevention of Money Laundering and Terrorist Financing (619/2019) lists the positions considered in Finland to be significant public positions referred to in chapter 1, section 4(11) of the AML Act.

GUIDELINE (paragraphs 180–184)

(180) According to the FIN-FSA's interpretation, supervised entities shall, in the risk assessment referred to in chapter 2, section 3 of the AML Act, assess the significance of political influence as part of risks associated with the customer relationship with a particular focus on the products and services provided and the geographical dimension.

(181) According to the FIN-FSA's interpretation, supervised entities shall prepare risk-based procedures to comply with the enhanced due diligence obligations referred to in chapter 3, section 13(2) of the AML Act. The procedures may vary for example depending on the product or service concerned.

[35] *Chapter 3, section (13)(3) of the AML Act.*

(182) According to the FIN-FSA's interpretation, the senior management of an obliged entity as referred to in chapter 3, section 13(3)(1) of the AML Act refers to a party with adequate information on ML/TF risks the supervised entity is exposed as well as adequate authority to make decisions with an influence on risks the supervised entity is exposed to.

(183) According to the FIN-FSA's interpretation, information concerning political influence shall be kept up to date and relevant in accordance with chapter 3, section 3 of the AML Act, which means that it is checked in regular intervals to monitor whether the person remains within the scope of enhanced due diligence obligation pertaining to politically exposed persons.

(184) The FIN-FSA recommends considering that specific regulation concerning politically exposed persons is based on objectives related to the prevention of corruption. Regulation concerning politically exposed persons should not be interpreted so that transactions involving politically exposed persons would always be considered suspicious as a rule. In accordance with preamble 33 of the Fourth Anti-Money Laundering Directive, refusing a business relationship with a person simply on the basis of the determination that he or she is a politically exposed person is contrary to the letter and spirit of said Directive and of the revised FATF Recommendations.

6.6.3 Enhanced due diligence obligation concerning a high-risk non-EEA country

(185) Chapter 3, section 13 a of the AML Act provides on enhanced procedures for transactions and payments relating to non-EEA Member States identified by the Commission as countries of high risk for money laundering and terrorist financing (high-risk third countries[36]).

(186) Chapter 3, section 13 a (1) of the AML Act lists customer due diligence procedures that shall be complied with by obliged entities, while subsection 2 lists actions that may be taken by the obliged entity following the risk-based assessment.

GUIDELINE (paragraphs 187–191)

(187) The FIN-FSA recommends that supervised entities consider paragraphs 4.55–4.57 of the EBA Risk Factors Guidelines in assessing whether a transaction or payment is associated with a high-risk country.

(188) According to the FIN-FSA's interpretation, the fact alone that a customer or beneficial owner thereof is a citizen of a high-risk country, does not oblige the supervised entity to comply with a procedure referred to in chapter 3, section 13 a of the AML Act, but the assessment shall take into account a broader set of facts pertaining to the customer and the transaction.

(189) According to the FIN-FSA's interpretation, supervised entities shall have procedures in place for the collection of information referred to in chapter 3, section 13 a of the AML Act. The supervised entity may determine what additional information to obtain, applying a risk-based approach.

(190) According to the FIN-FSA's interpretation, the senior management of an obliged entity as referred to in chapter 3, section 13 a (1)(5) of the AML Act refers to a party with adequate information on ML/TF risks the supervised entity is exposed as well as adequate authority to make decisions with an influence on risks the supervised entity is exposed to.

[36] *Commission Delegated Regulation (EU) 2016/1675*

(191) According to the FIN-FSA's interpretation, a supervised entity shall prepare policies and procedures as referred to in chapter 2, section 3(2) to comply with the obligation under chapter 3, section 13 a (2) of the AML Act including determination of the circumstances where it considers necessary to apply these procedures.

6.7 Correspondent relationships

6.7.1 Scope of application of the chapter

(192) This chapter applies to credit institutions, financial institutions and payment institutions referred to in chapter 1, section 4(1)(16) of the AML Act and payment service providers referred to in section 7 and 7 a of the Payment Institutions Act.

6.7.2 Definition of a correspondent banking relationship and counterparty due diligence

(193) In accordance with chapter 1, section 4(1)(18) of the AML Act, a correspondent relationship means[37]:

- the provision of banking services by one bank as the correspondent to another bank as the respondent, including providing a current or other liability account and related services, such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;
- the relationships between and among credit institutions and financial institutions including where similar services are provided by a correspondent institution to a respondent institution, and including relationships established for securities transactions or funds transfers.

(194) Chapter 3, section 12 of the AML Act provides on an enhanced customer due diligence procedures to be applied in correspondent banking relationships with counterparties established in a non-EEA Member State,

(195) The FIN-FSA's authority to issue more detailed regulations on the procedures to be followed in customer due diligence and the management of risks posed by customers to the activities of a supervised entity is based on the following provisions: Section 39(4) of the Payment Institutions Act, chapter 15, section 18(4) of the Credit Institutions Act, chapter 12, section 3(4) of the Investment Services Act, chapter 12, section 10 of the AIFM Act, chapter 6, section 21(4) of the Insurance Companies Act and chapter 26, section 15(4) of the Mutual Funds Act

(196) For the purposes of regulations 198-199 and guidelines 200-204, a supervised entity refers to supervised entities falling within the scope of authority to issue regulations under paragraph 195 above.

(197) Guidelines 200-204 apply, in addition to credit and financial institutions, to payment institutions and payment service providers referred to in sections 7 and 7 a of the Payment Institutions Act.

REGULATION (paragraphs 198–199)

(198) In correspondent banking relationships and arrangements comparable to a correspondent banking relationship, with a payment institution or a payment service provider referred to in

[37] *Article 3(8)(a) and (b) of 4AMLD.*

section 7 and 7 a of the Payment Institutions Act as one or both of the parties (*arrangement comparable to correspondent banking relationship*), supervised entities shall apply customer due diligence procedures under chapter 3 of the AML Act, including the risk-based assessment of the customer relationship.

(199) A supervised entity must be able to demonstrate to the FIN-FSA the establishment of the correspondent banking relationship and the fact that it has adequate information on the counterparty as well as ML/TF risk associated with the counterparty and the correspondent banking relationship.

GUIDELINE (paragraphs 200–204)

(200) According to the FIN-FSA's interpretation, a financial institution (*finanssilaitos*) as referred to in chapter 1, section 4(1)(18) of the AML Act means a financial institution (*rahoituslaitos*) referred to in chapter 3, section 12 on the enhanced customer due diligence related to correspondent banking relationships. A financial institution is defined in chapter 4, section 1(16) of the AML Act.

(201) According to the FIN-FSA's interpretation, the procedures referred to in the chapter 2, section 3(2) of the AML Act include procedures to determine whether its relationship with a credit, financial or payment institution or a payment service provider referred to in sections 7 and 7 a of the Payment Institutions Act constitutes individual transactions or a correspondent banking relationship referred to in chapter 1, section 4(1)(18) of the AML Act or an arrangement comparable to a correspondent banking relationship as referred to in paragraph 193. At least, the procedures shall take risks related to the counterparty and the transaction into account.

(202) According to the FIN-FSA's interpretation, a correspondent banking relationship under chapter 1, section 4(1)(18) of the AML Act arises at least where the purpose is to provide service on a recurrent basis and the relationship is ongoing by nature. For example, a correspondent banking relationship arises always when a correspondent bank provides a payment account to a counterparty.

(203) According to the FIN-FSA's interpretation, a risk assessment under chapter 2, section 3 of the AML Act shall consider the ML/TF risks associated with correspondent banking relationships and the related risk management methods.

(204) The FIN-FSA recommends that, in their risk-based assessment, as regards correspondent banking relationships, supervised entities consider paragraphs 8.4–8.9 of the EBA Risk Factors Guidelines when evaluating factors that increase or decrease risk.

6.7.3 Correspondent banking relationship with a counterparty established in the EEA

(205) In accordance with chapter 3, section 10(1) of the AML Act, an obliged entity shall apply the enhanced customer due diligence procedure for example where, based on the risk assessment, it estimates a higher than ordinary risk of money laundering and terrorist financing to attach to the case.

(206) Guidelines 207–209 apply, in addition to credit and financial institutions, to payment institutions and payment service providers referred to in sections 7 and 7 a of the Payment Institutions Act.

(207) According to the FIN-FSA's interpretation, chapter 3, section 10(1) of the AML Act means that a supervised entity may, based on the assessment of risks related to a correspondent banking relationship, come to the conclusion that enhanced due diligence measures are required in respect of the counterparty even though it is established in the EEA.[38]

Example

An indication of elevated risk could be, for example, if the counterparty is located in an EEA member state which is placed on a list maintained by the FATF of countries with strategic deficiencies in their regimes to counter and investigate money laundering and terrorist financing and which have prepared an action plan with the FATF to eliminate these deficiencies[39]. However, this does not mean that enhanced due diligence measures should be automatically applied to the counterparty.

(208) According to the FIN-FSA's interpretation, if a supervised entity intends to enter into correspondent banking relationships, it shall, as part of the procedures referred to in chapter 2, section 3(2), prepare risk-based approaches to be followed in the correspondent banking relationship to obtain adequate information, including procedures to comply with the enhanced due diligence obligation.

(209) The FIN-FSA recommends that, in correspondent banking relationships with counterparties domiciled within the EEA, the supervised entity, applying a risk-based approach:

- obtains adequate information on the counterparty to understand what its business consists of and to ensure that the counterparty has effective procedures to ensure compliance with AML/CFT regulations
- assesses the reputation of the counterparty based on publicly available information
- assesses the quality of supervision targeted at the supervised entity in the country where it is domiciled.
- carefully identifies the beneficial owners and owners of the counterparty and assesses the risks pertaining to its ownership structure.

6.7.4 Correspondent banking relationship with a counterparty established outside EEA

(210) In accordance with chapter 3, section 12(1) of the AML Act, if a credit institution or financial institution concludes a contract on the handling of payments and other assignments (*correspondent banking relationship*) with a credit institution or financial institution established in a non-EEA Member State, the credit institution or financial institution shall, before concluding the contract, obtain sufficient information about the respondent institution to be able to understand its business.

(211) In accordance with chapter 3, section 12(2) of the AML Act, a credit institution or financial institution shall assess the correspondent institution's reputation, the quality of the supervision it

[38] *Government bill 236/2021, p. 63.*
[39] *This list is often referred to as the "grey list". When the FATF places a country under increased monitoring, it means that the country has undertaken to resolve the identified strategic shortcomings rapidly within agreed schedules and that it is under more intense scrutiny. The FATF does not require the application of enhanced due diligence obligation to these countries, but it encourages its member states to consider the observations made by the FATF in their risk assessment.*

performs and its anti-money laundering and anti-terrorist financing measures. The senior management of the credit institution or financial institution shall give its approval for the establishment of the correspondent banking relationship. The contract shall explicitly lay out the customer due diligence obligations to be fulfilled and the supply of relevant information relating to these to the respondent institution upon request.

(212) Furthermore, in accordance with chapter 3, section 12(4) of the AML Act, if an investment firm, payment institution, fund management company or alternative fund manager or insurance company concludes a contract on an arrangement equivalent to that in subsection 1, the provisions of chapter 3, section 12 shall be observed.

(213) In accordance with chapter 3, section 12(5) of the AML Act, credit institutions and financial institutions shall, when offering payable-through accounts to other credit and financial institutions, ensure that the respondent credit or financial institution:

1) has identified its customers who have direct access to the account of the credit or financial institution and has performed the ongoing customer due diligence obligation in respect of these customers, and

2) supplies it, upon request, with the relevant customer due diligence data.

(214) Guidelines 215–219 apply, in addition to credit and financial institutions, to payment institutions and payment service providers referred to in sections 7 and 7 a of the Payment Institutions Act.

GUIDELINE (paragraphs 215–219)

(215) The FIN-FSA recommends that supervised entities, in assessing the adequacy of information required to meet the enhanced due diligence obligation under chapter 3, section 12 of the AML Act, with a view to the provisions of guideline 8.17 of the EBA Risk Factors Guidelines.

(216) According to the FIN-FSA's interpretation, the requirement under chapter 3, section 12 of the AML Act to obtain sufficient information on the counterparty to understand its business and the requirement of a risk-based assessment under chapter 3, section 1(2) of the AML Act comprise at least the following actions:

- assessment of the reputation of the counterparty based publicly available information
- assessment of the risk of money laundering and terrorist financing, also including the risk related to corruption, in the domicile of the counterparty
- assessment of the quality of supervision targeted at the counterparty in the country where it is domiciled (for example based on assessment reports by the FATF, the IMF or other parties or by contacting the authority supervising the counterparty)
- obtaining adequate information to ascertain that the counterparty has effective procedures to ensure compliance with AML/CFT regulations
- careful identification of the beneficial owners and owners of the counterparty and assesses the risks pertaining to its ownership structure.

(217) The FIN-FSA recommends that supervised entities obtain information to comply with the enhanced customer due diligence obligation from reliable and independent sources and directly from the counterparty.

(218) According to the FIN-FSA's interpretation, chapter 3, section 12(2) of the AML Act entails the obligation to document both the establishment of a correspondent banking relationship and the approval of senior management for entering into the correspondent banking relationship.

(219) According to the FIN-FSA's interpretation, in circumstances where the correspondent provides payment accounts to other credit and financial institutions, relevant customer due diligence data referred to in chapter 3, section 12(5)(2) of the AML Act that shall be submitted to the correspondent, includes at least such information the counterparty's customers that may be necessary to comply with the obligation to obtain information under chapter 3, section 4(3) or the reporting obligation under chapter 4, section 1 of the AML Act.

6.7.5 Shell banks

(220) In accordance with chapter 3, section 12 of the AML Act, a credit institution or financial institution may not initiate or continue a correspondent banking relationship with an institution that is a shell bank or whose accounts may be used by shell banks.

(221) In accordance with chapter 1, section 4(1)(19) of the AML Act, a shell bank means a credit or financial institution or an institution engaged in operations that are comparable to the operations of a credit or financial institution, established in a jurisdiction in which it does not have a physical presence or meaningful mind and management, and which does not belong to a credit or financial institution group subject to public supervision or to another corresponding financial consortium.

GUIDELINE (paragraph 222)

(222) According to the FIN-FSA's interpretation, credit and financial institutions shall have adequate policies, procedures and control as referred to in chapter 2, section 3(2) means that to ensure that they do not enter into correspondent banking relationships with shell banks.

7 Ongoing monitoring of customer relationship and obligation to obtain information

7.1 Ongoing monitoring

(1) Ongoing monitoring is provided on in chapter 3, section 4(2) and (3) of the AML Act, and the maintenance of the up-to-datedness and relevance of customer due diligence data is provided on in chapter 3, section 3(1) of the AML Act.

(2) In accordance with chapter 3, section 4(2) of the AML Act, obliged entities shall arrange monitoring that is adequate in view of the nature and extent of the customers' activities, the permanence and duration of the customer relationship and the risks involved in order to ensure that the customers' activities are consistent with the entities' experience or knowledge of the customers and their activities.

(3) In accordance with chapter 3, section 4(3) of the AML Act, obliged entities shall pay particular attention to transactions which are unusual in respect of their structure or size or with regard to the size or office of the obliged entity. The same also applies in the event of transactions which lack an obvious economic purpose or are inconsistent with obliged entities' experience or knowledge of the customer. When necessary, steps shall be taken to establish the source of the funds involved in the transaction.

(4) In this chapter, IT systems-based monitoring refers to model risk management practices related to ongoing monitoring of a customer and transactions, where scenarios pre-determined by the obliged agent are utilised and used by the IT system to highlight customers and transactions for manual monitoring.[40]

(5) The FIN-FSA's authority to issue more detailed regulations on the procedures to be followed in customer due diligence and the management of risks posed by customers to the activities of a supervised entity is based on the following provisions: Section 39(4) of the Payment Institutions Act, chapter 15, section 18(4) of the Credit Institutions Act, section 13(4) of the Virtual Currency Providers Act, chapter 12, section 3(4) of the Investment Services Act, chapter 12, section 10 of the AIFM Act, chapter 6, section 21(4) of the Insurance Companies Act, chapter 26, section 15(4) of the Act on Common Funds and chapter 8, section 13 of the Act on the Book-Entry System and Settlement Operations.

(6) For the purposes of regulations 17–21, a supervised entity refers to supervised entities falling within the scope of authority to issue regulations under paragraph 5 above.

GUIDELINE (paragraphs 7–16)

(7) According to the FIN-FSA's interpretation, the policies and procedures referred to in chapter 2, section 3(2) of the AML Act also include the procedures under chapter 3, section 4 of the AML Act to comply with the ongoing monitoring obligations.

(8) According to the FIN-FSA's interpretation, ongoing monitoring as referred to in chapter 3, section 4(2) of the AML Act includes the scrutiny of transactions undertaken throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the

[40] *On model risk management practises see chapter 5.1.*

obliged entity's knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that the documents, data or information held are kept up-to-date.[41]

(9) According to the FIN-FSA's interpretation, by virtue of chapter 2, section 3(2) of the AML Act, in establishing their procedures for ongoing supervision, supervised entities shall consider the nature, size and extent of its activities as well as its ML/TF risks.

(10) According to the FIN-FSA's interpretation, chapter 3, section 4(2) of the AML Act entails that the ongoing monitoring procedures shall include procedures for comparing customer due diligence data and the customer's activities to information obtained by the supervised entity on the customer and its activities in establishing the customer relationship or during the customer relationship as well as information obtained in the context of ongoing monitoring on the customer and its activities.

(11) According to the FIN-FSA's interpretation, ongoing monitoring referred to in chapter 2, section 4(2) of the AML Act entails that ongoing monitoring shall be systematic and comprehensive in proportion to the scope of the supervised entity's activities and the risk involved in the customer relationships. Comprehensive means, for example, that all products and services provided by the supervised entity have been taken into account in ongoing supervision.

(12) According to the FIN-FSA's interpretation, ongoing monitoring referred to in chapter 2, section 4(2) of the AML Act monitoring that is adequate in view of the risks means that the higher the ML/TF risk associated with the customer, the more effectively the supervised entity shall monitor the customer's activities and transactions and ensure that the activities are consistent with the information obtained on the customer (risk-based approach).

(13) According to the FIN-FSA's interpretation, the obligation under chapter 3, section 1(3) of the AML Act to observe customer due diligence measures throughout the course of the customer relationship on the basis of risk-based assessment entails, among other things, that the supervised entity shall assess the impact of changes in the customer's activities on its individual risk level, as part of the ongoing monitoring of the customer relationship and particularly when updating customer due diligence data.

(14) According to the FIN-FSA's interpretation, where a supervised entity making reports referred to in chapter 4, section 1(2) of the AML Act is concerned[42], ongoing monitoring shall include procedures for the detection of individual payments or remittances exceeding the threshold as well as the detection of interlinked payments or remittances.

(15) The FIN-FSA recommends that virtual currency providers have an IT systems-based analytical software at their disposal for customer due diligence and monitoring of customer activity if the nature and extent of the business pursued requires it, based on a risk assessment. Virtual currency providers should also use the information obtained by using the analytical software in assessing risks arising from customers to their activities.

(16) The FIN-FSA recommends that, if a virtual currency provider allows its customers to move virtual currencies into or from the service using features whose apparent purpose is to hide the origin of

[41] For more detailed information on the obtaining of customer due diligence information, see section 6.4 and on the updating of the customer due diligence information in particular section 6.4.4 and paragraph 138.
[42] See chapter 9.2 on threshold reporting

virtual currencies, this is taken into account in the risk assessment concerning the prevention of money laundering and terrorist financing and in organising ongoing monitoring. An example of a feature referred to herein is a so-called mixer.

REGULATION (paragraphs 17–21)

(17) Supervised entities shall ensure that adequate financial, technological and human resources are allocated to ongoing monitoring.

(18) Supervised entities shall organise ongoing monitoring so that they can detect and react without undue delay to unusual transactions as referred to in chapter 3, section 4(3) of the AML Act.

(19) Credit institutions and payment institutions, which as a rule have many customers and payment transactions, shall have IT systems-based monitoring in place for carrying out ongoing monitoring.

(20) Supervised entities shall ensure that both manual ongoing monitoring procedures and any IT systems-based monitoring scenarios at its disposal are based on the supervisor's risk assessment as referred to in chapter 2, section 3(1) of the AML Act and are sufficient with a view to the nature, size and extent of the business of the supervised entity. Particular attention shall be paid on risks concerning various products and services as well as customer relationship risks and geographical risks identified in the risk assessment.

(21) Supervised entities shall ensure that they have internal guidelines on ongoing monitoring as referred to in chapter 9, section 1(3) of the AML Act, covering at least:

- guidelines on the implementation of various ongoing monitoring duties with a view to risks associated with the supervised entity's different business areas as well as products and services
- guidelines on the careful and sufficient documentation of actions taken; in particular so as to demonstrate ex-post the actions taken as a result of ongoing monitoring findings (including the processing of monitoring hits) and the justifications of the actions.

GUIDELINE (paragraph 22)

(22) The FIN-FSA recommends that regulations 17–21 are also complied with by supervised entities excluded from the authority to issue regulations under paragraph 5.

7.2 Obligation to obtain information

(23) Chapter 3, section 4 of the AML Act provides on the obligation of obliged entities to obtain information concerning its customers and their transactions. According to said provision, obliged entities shall pay particular attention to transactions which are unusual in respect of their structure or size or with regard to the size or office of the obliged entity. The same also applies in the event of transactions which lack an obvious economic purpose or are inconsistent with obliged entities' experience or knowledge of the customer. When necessary, steps shall be taken to establish the source of the funds involved in the transaction.

(24) The FIN-FSA's authority to issue more detailed regulations on the procedures to be followed in customer due diligence and the management of risks posed by customers to the activities of a

supervised entity is based on the following provisions: Section 39(4) of the Payment Institutions Act, chapter 15, section 18(4) of the Credit Institutions Act, section 13(4) of the Virtual Currency Providers Act, chapter 12, section 3(4) of the Investment Services Act, chapter 12, section 10 of the AIFM Act, chapter 6, section 21(4) of the Insurance Companies Act, chapter 26, section 15(4) of the Act on Common Funds and chapter 8, section 13 of the Act on the Book-Entry System and Settlement Operations.

(25) For the purposes of regulation 26, a supervised entity refers to supervised entities falling within the scope of authority to issue regulations under paragraph 24 above.

REGULATION (paragraph 26)

(26) Supervised entities shall ensure that they have sufficient financial, technological and human resources to comply with the obligation to obtain information, including the examination of hits generated by information systems based monitoring.

GUIDELINE (paragraphs 27–33)

(27) The FIN-FSA recommends that regulation 26 is also complied with by supervised entities excluded from the authority to issue regulations under paragraph 24.

(28) According to the FIN-FSA's interpretation, the procedures referred to in chapter 2, section 3(2) of the AML Act, shall include the supervised entity's risk-based procedures to comply with the obligation to obtain information. The procedures shall indicate, among other things, what kind of clarification and supporting documents shall be obtained on the customer's transactions to resolve whether a notification referred to in chapter 4, section 1(1) of the AML Act should be made in respect of the transaction.

(29) The FIN-FSA recommends that, in assessing whether a transaction is unusual, supervised entities consider for example the following questions:

- Is the value of the transaction higher than usual relative to the typical activities of the customer or a certain customer group?
- Where are funds related to the transaction received from or transferred to, and is this consistent with the supervised entity's view of the typical activities of the customer or a certain customer group?
- Does the transaction allow the customer to receive payments from an unknown third party?
- Does the transaction involve geographical areas deviating from the customer's previous activities for example in terms of the point of service, or the origin or destination country of the payments?
- Are products or services being used differently from the customer's previous activities or in at a general level in a deviant manner compared to how the product or service is typically used?

(30) The FIN-FSA recommends that, in assessing unusual transactions, supervised entities use information from publicly available sources, where considered reliable and independent by the supervised entity.

(31) The FIN-FSA recommends that supervised entities reach out to the customer where necessary to obtain additional information on the purpose of the transaction or the customer's activity. However, a non-document explanation provided by the customer is not necessarily enough to eliminate a suspicion concerning a transaction or activity of the customer.

(32) The FIN-FSA recommends that, where necessary, supervised entities request written clarification from the customer, paying particular attention to the authenticity and reliability of the documents. For example, the following documents could be requested as a written clarification:

- contract of sale (property, apartment, car, boat or other valuable property)
- estate inventory documents (estate deed, partition deed, deed of estate distribution)
- customer's salary slip or tax decision
- business-related sale contracts, purchase and sale agreements, financing agreements, customs documents related to foreign trade and invoices
- promissory note

(33) According to the FIN-FSA's interpretation, establishing the source of the funds involved in the transaction as referred to in chapter 3, section 4(3) of the AML Act entails finding out the transaction to which the funds are related. To establish the source of funds, it is not enough that the supervised entity finds out from whom the funds originated or which credit institution or other payment service provider executed the funds transfer.

8 Refusal of customer relationship, restriction of services and termination of customer relationship

8.1 General

(1) The FIN-FSA has issued regulations and guidelines 7/2021, recommending compliance with the EBA Risk Factors Guidelines (EBA/GL/2021/02).

GUIDELINE (paragraph 2)

(2) The FIN-FSA recommends that also supervised entities other than those falling within the scope of application of regulations and guidelines 7/2021 comply with the EBA Risk Factors Guidelines when considering whether to refuse a new customer relationship or take measures to restrict services for existing customers or terminate a customer relationship.

8.2 Main principles for refusing a customer relationship, restricting services and terminating a customer relationship

(3) In accordance with chapter 3, section 1(1) of the AML Act, if an obliged entity is unable to carry out the customer due diligence measures laid down in chapter 3 of the AML Act, the entity may not establish a customer relationship, conclude a transaction or maintain a business relationship.

Where the obliged entity is a credit institution, it also may not execute a payment transaction through a payment account if it is unable to carry out the measures laid down for customer due diligence.

An obliged entity shall also assess whether it is necessary in this case to submit a suspicious transaction report. The obliged entity shall suspend the customer due diligence measures if, on reasonable grounds, it determines that the customer due diligence measures would endanger the submission of a suspicious transaction report.

(4) In accordance with chapter 3, section 1(1) of the AML Act, obliged entities shall ensure that all documents and data concerning customer due diligence and customer transactions are up to date and relevant.

(5) The FIN-FSA's authority to issue more detailed regulations on the procedures to be followed in customer due diligence and the management of risks posed by customers to the activities of a supervised entity is based on the following provisions: Section 39(4) of the Payment Institutions Act, chapter 15, section 18(4) of the Credit Institutions Act, section 13(4) of the Virtual Currency Providers Act, chapter 12, section 3(4) of the Investment Services Act, chapter 12, section 10 of the AIFM Act, chapter 6, section 21(4) of the Insurance Companies Act, chapter 26, section 15(4) of the Act on Common Funds and chapter 8, section 13 of the Act on the Book-Entry System and Settlement Operations.

(6) For the purposes of regulation 7-8, a supervised entity refers to supervised entities falling within the scope of authority to issue regulations under paragraph 5 above.

REGULATION (paragraphs 7–8)

(7) Supervised entities shall allow adequate time for customers to submit information before taking measures referred to in chapter 3, section 1(1) of the AML Act to restrict or terminate the customer relationship.

(8) The submission of due diligence data shall be possible by many different means taking into account among other things that not all customers necessarily have equal access to digital communication tools.

GUIDELINE (paragraphs 9–18)

(9) The FIN-FSA recommends that regulations 7–8 are also complied with by supervised entities excluded from the authority to issue regulations under paragraph 5.

(10) According to the FIN-FSA's interpretation, the measures referred to in chapter 3, section 1(1) of the AML Act provided for customer due diligence as referred to in chapter 3 of the AML Act do not only refer to measures taken by the supervised entity to obtain the minimum information provided in chapter 3, but also measures based on the obliged entity's own risk-based procedures for customer due diligence.

(11) The FIN-FSA recommends that supervised entities assess on a risk-sensitive basis how detailed data should be obtained for customer due diligence, where is the limit when customer due diligence data is adequate and when the supervised entity shall take measures referred to in chapter 3, section 1(1) of the AML to restrict services.

(12) According to the Government bill[43] services should not be restricted or payment instruments be blocked if the shortcoming in the customer due diligence data is not material and unavoidable, when considering actions provided on customer due diligence and risk-based customer assessments.

(13) According to the FIN-FSA's interpretation, when considering actions under chapter 3, section 1(1) of the AML Act, the termination of customer relationship should be the measure of last resort in circumstances where the supervised entity considers that it is not able to manage the ML/TF risk related to the customer relationship due to a reason referred to in chapter 3, section 1(1).

(14) The FIN-FSA recommends that, in circumstances where a customer fails to provide adequate customer due diligence data, the supervised entity shall primarily restrict services (for example by blocking a payment instrument) and terminate the contract only as a last resort. The need to terminate a customer relationship should be assessed in each individual case following a risk-based assessment.

(15) The FIN-FSA recommends that supervised entities assess risks related to customer relationships diversely and emphasising the significance of different risk factors, and also assess on a case-by-case basis how these risks can be managed before taking the restrictive measures referred to in chapter 3, section 1(1) of the AML Act.

(16) The FIN-FSA recommends considering that risks related to individual customer relationships also vary within the risk categories.

[43] *Government bill 228/2016, p. 102.*

(17) The FIN-FSA recommends supervised entities to note that applying a risk-based approach does not mean that supervised entities should refuse, or terminate, business relationships with entire categories of customers associated with high risk.[44]

(18) The FIN-FSA recommends that supervised entities implement appropriate measures to ensure that their procedures to comply with customer due diligence obligations do not lead to an undue denial of customers' access to financial services. In assessing whether restrictive measures are reasonable, any specific reasons should be considered as to why a customer has difficulties in providing requested information.

8.3 Financial inclusion perspective

GUIDELINE (paragraph 19)

(19) The FIN-FSA recommends that supervised entities assess the impacts of their activities, in addition to money laundering and terrorist financing, from the perspective of financial inclusion. In the assessment, attention should be paid on what kind of impacts there will be on a customer or category of customers if they are prevented from using certain products or services. The objective should be a balance of avoiding and mitigating risks on the one hand and providing a level playing field to economic activity in society on the other hand, particularly in respect of people in a vulnerable position.

8.4 Reason for deficiencies in customer due diligence data

GUIDELINE (paragraphs 20–22)

(20) According to the FIN-FSA's interpretation, in considering measures under chapter 3, section 1(1) of the AML Act, supervised entities shall also consider the reason for the incompleteness of customer due diligence data.

(21) The FIN-FSA recommends supervised entities to assess whether the termination of customer relationship with a private customer could lead to an undue outcome for the customer in circumstances where the incompleteness of customer due diligence data is due to a failure by the supervised entity itself in the retention of the data and where the customer has significant impediments to updating its data in a manner and schedule required by the supervised entity.

(22) The FIN-FSA recommends supervised entities to consider whether a private customer has a justified and credible reason for not being able to implement the customer due diligence measures and to assess the level of risk caused by the failure to implement the customer due diligence measures from the perspective of total risk associated with the customer relationship. In assessing the necessity of restrictive measures, supervised entities should also consider that the restrictive measures should not lead to the undue denial of access by private customers to financial services.

[44] *EBA Risk Factors Guidelines, guideline 4.9 on de-risking.*

8.5 Customer's difficulties in reverifying identity during a customer relationship

(23) In accordance with chapter 3, section 2(1)(4) of the AML Act, obliged entities shall identify their customers and verify their identities if they have doubts about the reliability or adequacy of previously obtained verification data on the identity of the customer.

(24) In accordance with chapter 3, section 1(3) of the AML Act, the customer due diligence measures laid down in chapter 3 of the AML Act shall be observed throughout the course of the customer relationship on the basis of risk-based assessment.

GUIDELINE (paragraphs 25–30)

(25) According to the FIN-FSA's interpretation, supervised entities shall verify the customer's identity again in accordance with chapter 3, section 2(1)(4) of the AML Act if the supervised entity has not, in connection with the establishment of the customer relationship, saved the information referred to in chapter 3, section 3(7) of the AML Act on the document used in the verification of identity or a copy of the document or information on the procedure or sources used in the verification, or if the information referred to in chapter 3, section 3(7) of the AML Act saved by the supervised entity has been lost.

(26) The FIN-FSA recommends supervised entities to assess whether the termination of customer relationship with a private customer could lead to an unreasonable outcome for the customer in circumstances where deficiencies in customer due diligence data pertaining to the verification of a private customer's identity are related to a failure by the supervised entity itself in the retention of the data and where the customer has significant impediments in the re-verification of identity in a manner and schedule required by the supervised entity.

(27) The FIN-FSA recommends supervised entities to assess whether the private customer has a justified and credible reason for not being able to re-verify identity and to assess the level of risk caused by the failure to re-verify identity from the perspective of overall risk associated with the customer relationship. In assessing the necessity of restrictive measures, supervised entities should also consider that the restrictive measures should not lead to the undue denial of access by private customers to financial services.

(28) According to the FIN-FSA's interpretation, the obligation under chapter 3, section 1(3) of the AML Act to apply the customer due diligence measures provided in chapter 3 to risk-based assessment throughout the duration of the customer relationship requires that the supervised entity implements adequate and commensurate risk management methods to mitigate risks due to inability to re-verify the identity of a customer or take restrictive actions referred to in chapter 3, section 1(1) of the AML Act since it would lead to undue denial of access to financial services by private customers.

(29) The FIN-FSA recommends that supervised entities consider, in circumstances referred to above in paragraph 27, the measures described in guideline 4.10 of the ESMA Risk Factors Guidelines to mitigate risks where a customer has legitimate and credible reasons for being unable to provide traditional forms of identity documentation. Such measures could include, for example:

- adjusting the level and intensity of monitoring in a way that is commensurate to the ML/TF risk associated with the customer, including the risk that a customer who may have provided a weaker form of identity documentation may not be who they claim to be; and

– offering only basic financial products and services, which restrict the ability of users to abuse these products and services for financial crime purposes. Where such basic products and services are concerned, it may also be easier for firms to identify unusual transactions or patterns of transactions, including the unintended use of the product. However, it is important that all restrictions are proportionate and do not unduly or unnecessarily limit customers' access to financial products and services.

(30) An application example related to FIN-FSA guidelines 27 and 28 above:

A supervised entity has had a longstanding customer relationship with a private customer. According to the supervised entity's assessment, the customer relationship does not involve elevated risk of money laundering or terrorist financing. In establishing the customer relationship – and potentially also several times during the customer relationship – the supervised entity has verified the identity of the private customer, but this data has not been retained in a manner compliant with the AML Act or the data has been lost, for example in connection with systems changes made by the supervised entity.

The supervised entity has requested the private customer to re-verify identity in accordance with chapter 3, section 2(1)(4) of the AML Act. However, the private customer is in a care facility and no longer has a valid proof of identity that could be used for the verification of identity, and due to health reasons has no possibility to visit the supervised entity in person. Neither does the private customer have the means to verify identity using strong electronic identification methods. The supervised entity has detected in ongoing monitoring that the customer's transactions are ordinary and often also regularly recurring (such as regular pension income and care facility charges).

If restrictive measures would lead to an undue denial of access to financial services by the private customer, and the restrictive measures could not be regarded as necessary from the perspective of total risk associated with the customer relationship based on the supervised entity's risk assessment, when taking into account the customer's justified and credible reasons for not being able to re-verify identity, the implementation of restrictive measures would not be due and commensurate. In these circumstances, the supervised entity shall assess, instead of restrictive measures, the level of risk that would arise if the verification of identity has not been renewed and take measures that are sufficient and commensurate to manage the risk.

9 Obligation to report to the Financial Intelligence Unit

9.1 Suspicious transaction report

(1) In accordance with chapter 4, section 1(1) of the AML Act, having fulfilled their obligation to obtain information provided in chapter 3, section 4(3) of the AML Act, obliged entities shall, without delay, report any suspicious transaction to the Financial Intelligence Unit referred to in the Act on the Financial Intelligence Unit. A suspicious transaction report shall be submitted irrespective of whether a customer relationship has been established or refused, and of whether the transaction has been carried out, suspended or refused.

(2) In accordance with chapter 4, section 5 of the AML Act, obliged entities shall suspend a transaction for further inquiries or refuse a transaction if:

1) the transaction is suspicious; or

2) the obliged entity suspects that the assets involved in the transaction are used for terrorist financing or a punishable attempt of such an act.

An obliged entity may carry out a transaction if it cannot be suspended or if its suspension or refusal is likely to frustrate efforts to determine the actual beneficiary of the transaction.

(3) Provisions on the right of the Financial Intelligence Unit to order the suspension of a transaction for a fixed period of time are laid down in section 6 of the Act on the Financial Intelligence Unit. Subsection 1 of said section provides that a policeman working as a commanding officer in the Financial Intelligence Unit may impose an order to an obliged entity to suspend a transaction for a maximum duration of 10 banking days, if such a suspension is necessary to prevent, detect, investigate, or to begin the investigation of, money laundering and terrorist financing and such crimes as were committed to gain the assets or proceeds of crime subject to money laundering or terrorist financing.

GUIDELINE (paragraphs 4–10)

(4) According to the FIN-FSA's interpretation, a supervised entity's procedures under chapter 2, section 3(2) shall include procedures applied by the supervised entity in detecting suspicious transactions, including procedures for processing suspicious transaction reports within the supervised entity and submitting reports to the Financial Intelligence Unit.

(5) According to the FIN-FSA's interpretation, the obligation referred to in chapter 4, section 1(1) of the AML Act to report suspicious transactions also applies to circumstances where suspicions are related to the customer and the customer's activities in general and not just an individual transaction.

(6) According to the FIN-FSA's interpretation, chapter 4, section 5 of the AML Act shall be applied in conjunction with chapter 3, section 4(3) on the obligation to obtain information and chapter 4, section 1(1) of the AML Act so that the nature of the suspicious transaction determines the timing and sequence of compliance with the obligation to obtain information, compliance with the reporting obligation as well as the suspension and refusal of a transaction.

(7) According to the FIN-FSA's interpretation, having detected an unusual transaction referred to in chapter 3, section 4(3) of the AML Act, the supervised entity may suspend the transaction in

accordance with chapter 4, section 5 of the AML Act for the duration required by compliance with the obligation to obtain information, where this is feasible and does make the identification of the beneficiary of the transaction more difficult.

(8) According to the FIN-FSA's interpretation, a transaction suspended under chapter 4, section 5 of the AML Act for the duration required by compliance with the obligation to obtain information shall be kept suspended or refused when a report referred to in chapter 4, section 1 of the AML Act is made, provided that the suspension or refusal is feasible and does not make the identification of the beneficiary of the transaction more difficult.

(9) According to the FIN-FSA's interpretation, a suspicious transaction report referred to in chapter 4, section 1 of the AML Act shall be made to the Financial Intelligence Unit also in circumstances where the suspicious transaction is detected afterwards, or issues making the transaction suspicious arise afterwards.

(10) The FIN-FSA recommends that, in complying with the obligation to obtain information, the supervised entity contacts the Financial Intelligence Unit to find out to what extent the suspension or refusal of a transaction would make it more difficult to identify the beneficiary of the transaction.

9.2 Threshold report

(11) In accordance with chapter 4, section 1(2) of the AML Act, obliged entities may submit suspicious transaction reports also on payments or other remittances, carried out individually or in several linked operations, that exceed the maximum threshold established by them. However, money remittance service providers referred to in section 1, subsection 2, paragraph 5 of the Act on Payment Institutions shall report every payment or remittance that has a value of at least EUR 1,000, whether carried out individually or in a number of linked operations.

(12) In this chapter, a threshold value report refers to the reports under chapter 4, section 1(2) of the AML Act to the Financial Intelligence Unit.

GUIDELINE (paragraphs 13–15)

(13) According to the FIN-FSA's interpretation, threshold reporting referred to in chapter 4, section 1(2) of the AML Act complements the procedure of suspicious transaction reporting, and when an obliged entity makes a threshold report, it does not mean that it would not also have to report circumstances referred to in chapter 4, section 1(1) of the AML Act.

(14) According to the FIN-FSA's interpretation, the decision referred to in chapter 4, section 1(2) of the AML Act by a supervised entity other than those referred to in section 1(2)(5) of the Payment Institutions Act to introduce the threshold reporting procedure and establish a threshold shall be based on the supervised entity's risk assessment.

(15) According to the FIN-FSA's interpretation, supervised entities making threshold reports shall define in the procedures referred to in chapter 2, section 3(2) of the AML Act what they consider linked payments or remittances as referred to in chapter 4, section 1(2) of the AML Act and define procedures to detect such payments and remittances (see chapter 7.1, paragraph 14).

9.3 Form and content of report

(16) In accordance with chapter 4, section 2(1) of the AML Act, suspicious transaction reports shall be submitted electronically by using the application provided by the Financial Intelligence Unit for this purpose. For specific reasons, reports may also be submitted by using another encrypted connection or secure procedure.[45]

(17) In accordance with chapter 4, section 2(2) of the AML Act, suspicious transaction reports shall contain the due diligence data referred to in chapter 3, section 3 of the AML Act, as well as details of the nature of the transaction, the amount and currency of the funds or other assets involved in the transaction, the source or target or the funds or other assets, and the reasons for considering the transaction suspicious, as well as information on whether the transaction was carried out, suspended or refused.

(18) In accordance with chapter 4, section 1(4) of the AML Act, obliged entities shall provide, free of charge, the Financial Intelligence Unit with all data, information and documents necessary to investigate the suspicion. Obliged entities shall respond to the Financial Intelligence Unit's requests for information within the reasonable period of time determined by the Financial Intelligence Unit.

GUIDELINE (paragraphs 19-21)

(19) The FIN-FSA recommends that the supervised entity reports suspicious transactions in a manner allowing the Financial Intelligence Unit to assess the sequence of events and actions taken by the supervised entity in respect of the matter. The report should be written clearly and objectively.

(20) The FIN-FSA recommends that, in the suspicious transaction report, the supervised entity states its opinion about whether the suspicion concerns the customer or whether the supervised entity suspects is customer has fallen victim to a suspicious transaction.

(21) The FIN-FSA recommends that a supervised entity with different products and services indicates in the report the business area or product category where the suspicious transaction was detected.

9.4 Retention of information concerning suspicious transactions and secrecy obligation concerning the information

(22) Chapter 4, section 3 of the AML Act provides on the retention of information concerning suspicious transactions.

(23) Chapter 4, section 4 of the AML Act provides on the secrecy obligation concerning suspicious transactions and related exceptions.

(24) In accordance with chapter 4, section 4(1) of the AML Act, obliged entities may not disclose the submission or investigation of a report to the suspect or to any other party. The secrecy obligation also applies to the employees of obliged entities and to parties which have obtained information subject to a secrecy obligation pursuant to this section.

[45] *The Financial Intelligence Unit's electronic application, GoAML, is available at https://ilmoitus.rahanpesu.fi/Home*

GUIDELINE (paragraphs 25–28)

(25) According to the FIN-FSA's interpretation, supervised entities' procedures referred to in chapter 2, section 3(2) of the AML Act shall include procedures for the retention of information and documents pertaining to submitted suspicious transaction reports and for checking the necessity of retention. Particular attention should be paid to the obligation to keep information and document separate from the customer register.

(26) According to the FIN-FSA's interpretation, the purpose of the secrecy obligation provided in chapter 4, section 4(1) of the AML Act is to ensure that information concerning suspicious transactions is not revealed to the person under suspicion or a third party outside the obliged entity.

(27) According to the FIN-FSA's interpretation, supervised entities' procedures referred to in chapter 2, section 3(2) of the AML Act shall include procedures for complying with the secrecy obligation concerning suspicious transactions, including procedures to apply exemptions from the secrecy obligation.

(28) The FIN-FSA recommends that supervised entities ensure that information concerning suspicious transaction is accessible within the organisation only to parties whose duties require so.

10 Fulfilment of customer due diligence obligations on behalf of obliged entities and outsourcing of duties

10.1 Difference between using a third party and outsourcing

(1) Chapter 3, section 7 of the AML Act provides on the possibilities of the supervised entity to use a so-called third party in fulfilling its customer due diligence obligations.[46]

(2) Chapter 3, section 7(8) of the AML Act provides that obliged entities are not exempt from the responsibilities under this Act on the grounds that customer due diligence obligations have been fulfilled by a third party on their behalf.

(3) Chapter 3, section 15 of the AML Act provides that the provisions of chapter 3 concerning third parties and enhanced customer due diligence do not apply if the obliged entity has outsourced its customer due diligence or uses a representative on the basis of a contractual relationship and the outsourced service provider or representative is to be regarded as part of the obliged entity.[47]

GUIDELINE (paragraphs 4–7)

(4) According to the FIN-FSA's interpretation, chapter 3, section 7 of the AML Act corresponds to section 11 of the old AML Act.

(5) In accordance with the Government bill[48], section 11 of the old AML Act provided that customer due diligence obligations may be fulfilled by a third party on behalf of the obliged entity. Where customer due diligence obligations have already been fulfilled once in compliance with said Act, subject to certain preconditions, the obliged entity does not have to perform the same customer due diligence obligations again. The section does not apply to outsourcing or agency relationships where the provider of the outsourcing service or the agent can be considered part of the obliged entity based on a contractual relationship. Hence, the AML Act does not regulate to what kind of parties the performance of customer due diligence measures may be contractually assigned.

(6) According to the FIN-FSA's interpretation, chapter 3, section 7 of the AML Act does not concern outsourcing or agency relationships, and the AML Act does not provide on procedures to be applied in outsourcing or agency relationships.

(7) According to the FIN-FSA's interpretation, the provisions of chapter 3, section 7 of the AML Act on the use of third parties also apply to outsourcing or the use of a representative, which means that supervised entities cannot be released by contractual relationships from responsibilities imposed on them in the AML Act.

10.2 Use of a third party

(8) In accordance with chapter 3, section 7(1) of the AML Act, customer due diligence obligations may be fulfilled on behalf of obliged entities by another obliged entity referred to in chapter 1, section 2, subsection 1 or by an equivalent operator authorised or registered in another EEA

[46] *Article 25–28 of 4AMLD.*
[47] *Article 29 of 4AMLD.*
[48] *Government bill 25/2008, p. 48.*

Member State (*third party*) when the operator is subject to customer due diligence and data retention obligations equivalent to those laid down in this Act and when compliance with those obligations is supervised.

(9) In accordance with chapter 3, section 7(2)(1) of the AML Act, customer due diligence obligations may also be fulfilled by an operator that is equivalent to the obliged entity and is authorised or registered in a non-EEA State if the operator is subject to customer due diligence and data retention obligations equivalent to those laid down in this Act and compliance with those obligations is supervised. It is also required that the operator equivalent to an obliged entity has been established in a State whose system for preventing and investigating money laundering and terrorist financing, in the estimation of the Commission, does not pose a significant risk to the EU's internal market.[49]

(10) In accordance with chapter 3, section 7(3) of the AML Act, an obliged entity cannot accept the following as a third party:

- a payment institution which provides the money remittance referred to in the Act on Payment Institutions as a primary payment service;
- a natural or legal person referred to in section 7 or 7a of the Act on Payment Institutions; or
- a party engaging in currency exchange.[50]

(11) In accordance with chapter 3, section 7(4) of the AML Act, obliged entities shall ensure that before carrying out a transaction they receive from the third party the data referred to in section 3, subsection 2, paragraphs 1–7 of the AML Act. In addition, obliged entities shall ensure that customer due diligence data are available to them and that the third party submits the data to them upon request.

(12) In accordance with chapter 3, section 7(7) of the AML Act, obliged entities shall subject to ongoing monitoring in the manner referred to in section 4, subsection 2 any customer relationships where customer due diligence obligations have been carried out by a third party.

(13) In accordance with chapter 3, section 7(8) of the AML Act, obliged entities are not exempt from the responsibilities under the AML Act on the grounds that customer due diligence obligations have been fulfilled by a third party on their behalf.

GUIDELINE (paragraphs 14–21)

(14) According to the FIN-FSA's interpretation, if a supervised entity intends to use a third party to perform its obligations concerning customer due diligence, the procedures referred to in chapter 2, section 3(2) of the AML Act shall include procedures to comply with the obligations provided in chapter 3, section 7 of the AML Act. Special attention shall be paid in the procedures to ensuring the fulfilment of requirements on the submission of information under chapter 3, section 7(4) of the AML Act.

(15) According to the FIN-FSA's interpretation, a supervised entity may use a third party in ways referred to in chapter 3, section 7(1) and (2) of the AML Act only in circumstances where a natural

[49] *The list under Commission Regulation 2016/1675 of third-country jurisdictions which have strategic deficiencies in their anti-money laundering and countering the financing of terrorism regimes that pose significant threats to the financial system of the Union ('high-risk third countries').*
[50] *Parties engaging in currency exchange refer to foreign exchange agencies registered in the anti-money laundering supervision register of the Regional State Administrative Agency (AVI).*

or legal person is the third party's customer and also is or will be the supervised entity's customer, and where the third party has already completed customer due diligence measures in respect of the customer. Thus, the supervised entity may use again information obtained by the third party on the customer.

(16) According to the FIN-FSA's interpretation, a third party referred to in chapter 3, section 7(1) and (2) of the AML Act does not have to be the same kind of operator as the supervised entity itself. For example, a credit institution may use information received from an investment service provider for customer due diligence.

(17) According to the FIN-FSA's interpretation, customer due diligence obligations referred to in chapter 3, section 7 that may be fulfilled by a third party, as referred to in the provision, on behalf of the obliged entity only refer to:

- Customer identification and identity verification as referred to in chapter 3, section 2 of the AML Act
- Identification and identity verification as referred to in chapter 3, section 6 of the AML Act, of a beneficial owner
- Information referred to in chapter 3, section 4(1) of the AML Act on customers' and their beneficial owners' activities, the nature and extent of their business, and the grounds for the use of the service or product.[51]

(18) According to the FIN-FSA's interpretation, risk-based assessment of the customer relationship as referred to in chapter 3, section 1 of the AML Act does not fall within the scope of customer due diligence obligations referred to in chapter 3, section 7 of the AML Act which may be performed by a third party on behalf of the supervised entity.

(19) According to the FIN-FSA's interpretation, supervised entities shall comply with their own customer due diligence procedures referred to in chapter 2, section 3(2) of the AML Act also when using a third party referred to in chapter 3, section 7 of the AML Act. Hence, the supervised entity itself shall for example obtain additional information on the customer and its activity if information received from the third party does not meet the requirements posed by the supervised entity in its procedures to fulfil the enhanced due diligence obligation referred to in chapter 3, section 10 of the AML Act.

(20) According to the FIN-FSA's interpretation, when assessing the fulfilment of the requirements of chapter 3, section 7(1) and (2) of the AML Act, supervised entities shall obtain adequate information on the third party to evaluate whether it meets the requirements concerning customer due diligence procedures and data retention.

(21) The FIN-FSA recommends that where a supervised entity recurrently uses a third party to fulfil the customer due diligence obligation, it conducts regular audits to ensure the adequacy of data collected on the customers by the third party. In addition, the supervised entity should check on a regular basis that the information is available at its request.

[51] *Articles 13 and 25 of 4AMLD.*

10.3 Use of a third party domiciled in a high-risk third country within the group or other financial consortium

(22) Chapter 3, section 7(5) of the AML Act provides on the conditions subject to which an obliged entity may use as a third party another obliged entity domiciled in a high-risk third country as referred to in chapter 3, section 7(2) of the AML Act[52]. The use of a third party domiciled in a high-risk third country always requires the FIN-FSA's approval.

(23) In accordance with chapter 3, section 7(5) of the AML Act, the supervisory authority may consider the conditions relating to the third party laid down in this section to be fulfilled if:

1) the obliged entity obtains the data from a third party which belongs to the same group or other consortium as the obliged entity;

2) the group or consortium complies with internal procedures common to the group or consortium and equivalent to the provisions of this Act concerning customer due diligence, data retention, and the prevention and detection of money laundering and terrorist financing;

3) compliance with paragraph 2 is monitored by the supervisory authority of the home state of the parent company of the group or other financial consortium; and

4) risk management and risk reduction relating to states with a high risk of money laundering and terrorist financing have been appropriately taken into account in the procedures of the group or other financial consortium concerning prevention and detection of money laundering and terrorist financing.

(24) The FIN-FSA's authority to issue more detailed regulations on the procedures to be followed in customer due diligence and the management of risks posed by customers to the activities of a supervised entity is based on the following provisions: Section 39(4) of the Payment Institutions Act, chapter 15, section 18(4) of the Credit Institutions Act, section 13(4) of the Virtual Currency Providers Act, chapter 12, section 3(4) of the Investment Services Act, chapter 12, section 10 of the AIFM Act, chapter 6, section 21(4) of the Insurance Companies Act, chapter 26, section 15(4) of the Act on Common Funds and chapter 8, section 13 of the Act on the Book-Entry System and Settlement Operations.

(25) For the purposes of regulation 26, a supervised entity refers to supervised entities falling within the scope of authority to issue regulations under paragraph 24 above.

REGULATION (paragraph 26)

(26) A supervised entity shall obtain the FIN-FSA's approval before beginning to use a third party domiciled in a high-risk third country to fulfil its customer due diligence obligations. The application shall include a statement by the supervised entity concerning the fulfilment of obligations provided in chapter 3, section 7(5) of the AML Act.

[52] *Article 26(2) of 4AMLD.*

GUIDELINE (paragraphs 27–28)

(27) According to the FIN-FSA's interpretation, also within a consolidation group or other financial consortium, customer due diligence obligations referred to in chapter 3, section 7 that may be fulfilled by a third party as referred to in the provision, on behalf of the obliged entity only refer to:

- Customer identification and identity verification as referred to in chapter 3, section 2 of the AML Act
- Identification and identity verification as referred to in chapter 3, section 6 of the AML Act, of a beneficial owner
- Information referred to in chapter 3, section 4(1) of the AML Act on customers' and their beneficial owners' activities, the nature and extent of their business, and the grounds for the use of the service or product.[53]

(28) According to the FIN-FSA's interpretation, also within a group or other financial consortium, risk-based assessment of the customer relationship as referred to in chapter 3, section 1 of the AML Act does not fall within the scope of customer due diligence obligations referred to in chapter 3, section 7 of the AML Act which may be performed by a third party on behalf of the supervised entity.

10.4 Outsourcing based on a contractual relationship

GUIDELINE (paragraphs 29–32)

(29) The EBA has issued Guidelines on outsourcing arrangements (EBA/GL/2019/02) for credit institutions, payment institutions and e-money issuers.

(30) The FIN-FSA has issued regulations and guidelines 1/2012 Outsourcing in supervised entities belonging to the financial sector.[54]

(31) According to the FIN-FSA's interpretation, supervised entities shall, in the risk assessment referred to in chapter 2, section 3 of the AML Act, assess risks related to outsourcing and the use of an agent and also take outsourcing and the use of an agent into account in preparing the policies, procedures and controls referred to in chapter 2, section 3(2) of the AML Act if they intend to outsource duties related to compliance with the obligations of the AML Act or use an agent to fulfil the obligations.

(32) The FIN-FSA recommends that supervised entities do not outsource outside the group or financial consortium the following duties related to compliance with the AML Act:

- arrangement of the policies, procedures and controls referred to in chapter 2, section 3(2) of the AML Act and the approval of these policies, procedures and controls referred to in chapter 2, section 3(3) of the AML Act
- principles to be applied in the risk-based assessment referred to in chapter 3, section 1(2) of the AML Act, including principles applied in model risk management practices, and approval thereof

[53] *Articles 13 and 25 of 4AMLD.*
[54] *The FIN-FSA regulations and guidelines on outsourcing are being updated, and the references will be aligned with the new regulations and guidelines, once these have been published.*

- preparation and approval of procedures related to the ongoing monitoring referred to in chapter 3, section 4(2) of the AML Act and to the obligation to obtain information referred to in paragraph (2) of said section
- preparation and approval of procedures concerning the detection and reporting of suspicious transactions referred to in chapter 4, section 1 of the AML Act.

11 Reporting to FIN-FSA

(1) In accordance with chapter 2, section 2(1)(3) of the AML Act, in preparing the supervisor-specific risk assessment, the FIN-FSA shall have regard to the risks of money laundering and terrorist financing concerning the sector supervised by them and relating to the obliged entities and to their customers, products and services.

(2) In accordance with chapter 2, section 2(2) of the AML Act, in determining the scope and frequency of supervision, the FIN-FSA shall also have regard to the sector risks referred to in chapter 2, section 2(1)(3) of the AML Act.

(3) In accordance with chapter 7, section 2(1) of the AML Act, the FIN-FSA shall have the right to obtain the information and reports requested by it to enable the performance of the duties referred to in the AML Act or in provisions issued under it.

(4) In accordance with chapter 9, section 6(2) of the AML Act, the FIN-FSA may issue regulations concerning the regular submission to it, and manner of submission, of information concerning the internal supervision of the prevention of money laundering and terrorist financing and the risk management carried out by an obliged entity under its supervision.

REGULATION (paragraphs 5–6)

(5) Supervised entities shall submit the information required by the FIN-FSA for the assessment of ML/TF risks under the RA-reporting framework valid at the time on the RA-reporting template available in the Jakelu distribution service.[55]

(6) Supervised entities shall submit the information referred to in paragraph 5 to the FIN-FSA on an annual basis by 28 February.

GUIDELINE (paragraphs 7–8)

(7) The FIN-FSA recommends that supervised entities prepare a declaration of the accuracy of the information reported pursuant to these regulations and guidelines. The declaration should be dated, and it should be signed both by the person preparing the report and the person verifying the data. The supervised entity should keep the signed declaration and present it to the FIN-FSA at request. The supervised entity should prepare the declaration in connection with the first report, and updates are whenever changes take place in the process described in it.

(8) The FIN-FSA recommends that, in preparing the declaration referred to above in paragraph 7, the guidance available in the Reporting section of the FIN-FSA's website (www.finanssivalvonta.fi) is observed.

[55] *The reporting map for the financial and insurance sectors is available in the Reporting section of the FIN-FSA website (www.finanssivalvonta.fi).*

12 Repealed regulations and guidelines

These regulations and guidelines repeal the following FIN-FSA regulations and guidelines as well as statements:

- Standard 2.4 (Customer due diligence - Prevention of money laundering and terrorist financing)
- FIN-FSA statement on customer due diligence information and banks' code of conduct 3/2016).
- FIN-FSA statement on simplified customer due diligence procedures for private road maintenance associations and public water area maintenance associations (27/2020)