

Issuer:	Riigikogu
Type:	act
In force from:	16.07.2016
In force until:	05.07.2017
Translation published:	11.07.2016

Money Laundering and Terrorist Financing Prevention Act¹

Passed 19.12.2007
RT I 2008, 3, 21
Entry into force 28.01.2008

Amended by the following acts

Passed	Published	Entry into force
04.06.2008	RT I 2008, 27, 177	10.07.2008
06.05.2009	RT I 2009, 27, 164	08.06.2009
26.11.2009	RT I 2009, 61, 401	26.12.2009
26.11.2009	RT I 2009, 62, 405	01.01.2010
17.12.2009	RT I 2010, 2, 3	22.01.2010
22.04.2010	RT I 2010, 22, 108	01.01.2011, will enter into force on the date specified in the decision of the Council of the European Union concerning abrogation of the derogation established with regard to the Republic of Estonia on the basis of Article 140 (2) of the Treaty on the Functioning of the European Union, Decision No. 2010/146/EU of the Council of the European Union of 13 July 2010 (OJ L 196, 28.07.2010, pp. 24-26).
12.05.2010	RT I 2010, 26, 129	05.10.2010
23.02.2011	RT I, 25.03.2011, 1	01.01.2014; date of entry into force amended to 01.07.2014 [RT I, 22.12.2013, 1]
09.06.2011	RT I, 29.06.2011, 1	30.06.2011, in part 09.07.2011
16.06.2011	RT I, 08.07.2011, 6	18.07.2011
08.12.2011	RT I, 29.12.2011, 1	01.01.2012, in part 01.01.2014 and 01.11.2014; date of entry into force partially amended to 01.07.2014 [RT I, 22.12.2013, 1]
18.04.2012	RT I, 08.05.2012, 1	18.05.2012
05.12.2013	RT I, 22.12.2013, 1	01.01.2014
19.02.2014	RT I, 13.03.2014, 4	01.07.2014
05.06.2014	RT I, 29.06.2014, 1	01.07.2014
19.06.2014	RT I, 29.06.2014, 109	01.07.2014
19.06.2014	RT I, 12.07.2014, 1	01.01.2015
19.06.2014	RT I, 29.06.2014, 109	01.07.2014, the ministers' official titles have been replaced on the basis of subsection 107 ³ (4) of the Government of the Republic Act.
11.02.2015	RT I, 12.03.2015, 1	01.01.2016
18.02.2015	RT I, 19.03.2015, 2	29.03.2015
18.02.2015	RT I, 19.03.2015, 4	29.03.2015
16.12.2015	RT I, 31.12.2015, 38	10.01.2016

Chapter 1 GENERAL PROVISIONS

Division 1 Purpose and Scope of Application of Act

§ 1. Purpose of Act

The purpose of this Act is to prevent the use of the financial system and economic space of the Republic of Estonia for money laundering and terrorist financing.

§ 2. Scope of application of Act

(1) This Act regulates:

- 1) the taking of due diligence measures by obligated persons for prevention of money laundering and terrorist financing;
- 2) the supervision exercised over obligated persons in complying with this Act;
- 3) the bases of operation of the Financial Intelligence Unit;
- 4) the liability of obligated persons for violations of the requirements arising from this Act.

(2) The provisions of the Administrative Procedure Act apply to administrative proceedings prescribed in this Act, taking account of the specifications provided for in this Act.

§ 3. Application of Act

(1) This Act applies to the economic or professional activities of the following persons:

- 1) credit institutions;
- 2) financial institutions;
- 3) organisers of games of chance;
- 4) persons who carry out or act as intermediaries in transactions with real property;
- 5) traders for the purposes of the Trading Act, if a cash payment of more than 15 000 euros or an equal amount in another currency is made to the trader, regardless of whether the financial obligation is performed in the transaction in a single payment or in several linked payments, unless otherwise provided by law;
[RT I, 08.05.2012 – entry into force 18.05.2012]
- 6) pawnbrokers;
- 6¹) persons engaged in the buying-in or wholesale of precious metals, precious metal articles or precious stones, except precious metals and precious metal articles used for production, scientific or medical purposes;
[RT I, 08.05.2012, 1 – entry into force 18.05.2012]
- 7) auditors and providers of accounting services;
- 8) providers of accounting or tax advice services;
- 9) providers of trust and company services;
- 10) non-profit associations and foundations for the purposes of the Non-profit Associations and Foundations Act, if a cash payment of more than 15 000 euros or an equal amount in another currency is made to them, regardless of whether the financial obligation is performed in the transaction in a single payment or in several linked payments, unless otherwise provided by law.
[RT I, 08.05.2012 – entry into force 18.05.2012]

(2) This Act applies to notaries, attorneys, enforcement officers, bankruptcy trustees, interim bankruptcy trustees and providers of other legal services if they act in the name and on account of a customer in financial or real property transactions. This Act also applies to the specified persons if they guide the planning or making of a transaction or perform a professional operation or provide a professional service, which involves the following:

- 1) the purchase or sale of immovables, enterprises or shares of companies;
[RT I 2009, 61, 401 – entry into force 26.12.2009]
- 2) the management of the customer's money, securities or other property;
- 3) the opening or managing of bank accounts or security accounts;
- 4) the acquisition of funds necessary for the foundation, operation or management of companies;
- 5) the foundation, operation or management of trusts, companies or other similar entities.
[RT I 2009, 27, 164 – entry into force 08.06.2009]

(2¹) This Act applies to the registrar of the Estonian Central Register of Securities if it organises opening securities accounts and provides services relating to register operations without mediation by an account administrator.

[RT I 29.06.2011 – entry into force 09.07.2011]

(3) For the purposes of this Act ‘cash’ means cash within the meaning of Regulation (EC) No. 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community (OJ L 309, 25.11.2005, pp. 9-12). The provisions regarding cash are also applicable to performance of financial obligations using a precious metal, which is measured in bars or other units.

(4) For the purposes of this Act, ‘precious stones’ means natural and artificial precious stones and semi-precious stones, their powder and dust, and natural and cultivated pearls. In this Act the terms ‘precious metal’ and ‘precious metal articles’ are used within the meaning set out in the Precious Metal Articles Act. [RT I, 08.05.2012, 1 – entry into force 18.05.2012]

Division 2 Definitions

§ 4. Money laundering

(1) Money laundering means:

- 1) the concealment or disguise of the true nature, source, location, disposition, movement, right of ownership or other rights related to property derived from criminal activity or property obtained instead of such property;
- 2) the conversion, transfer, acquisition, possession or use of property derived from criminal activity or property obtained instead of such property for the purpose of concealing or disguising the illicit origin of the property or of assisting a person who is involved in criminal activity to evade the legal consequences of his or her action.

(2) Money laundering also means a situation whereby the criminal activity that generated the property to be laundered was carried out in the territory of another state.

§ 5. Terrorist financing

Terrorist financing means financing acts of terrorism as defined in § 237³ of the Penal Code.

§ 6. Credit institutions and financial institutions

(1) For the purposes of this Act, ‘credit institution’ means:

- 1) a credit institution within the meaning of the Credit Institutions Act;
- 2) the branch of a foreign credit institution registered in the Estonian commercial register.

(2) For the purposes of this Act, ‘financial institution’ means:

- 1) a provider of currency exchange services;
 - 2) a payment service provider within the meaning of the Payment Institutions and Electronic Money Institutions Act;
 - 3) an electronic money institution within the meaning of the Payment Institutions and Electronic Money Institutions Act;
 - 4) a provider of services of alternative means of payment;
 - 5) an insurer engaged in life assurance within the meaning of the Insurance Activities Act (hereinafter *insurer*);
 - 6) an insurance broker engaged in mediation of life assurance within the meaning of the Insurance Activities Act (hereinafter *insurance broker*);
 - 7) a management company and an investment fund established as a public limited company within the meaning of the Investment Funds Act;
 - 8) an investment firm within the meaning of the Securities Market Act;
 - 9) a savings and loan association within the meaning of the Savings and Loan Associations Act;
 - 10) another financial institution within the meaning of the Credit Institutions Act;
 - 11) the branch of a foreign service provider registered in the Estonian commercial register and providing a service specified in clauses 1) to 10).
- [RT I 2010, 2, 3 – entry into force 22.01.2010]

(3) For the purposes of this Act, a currency exchange service is the exchange of the official currency of one country for the official currency of another country within economic or professional activities of an undertaking.

(4) A provider of services of alternative means of payment is a person who in its economic or professional activities and through a communications, transfer or clearing system buys, sells or mediates funds of monetary value by which financial obligations can be performed or which can be exchanged for an official currency, but who is not a person specified in subsection (1) or a financial institution for the purposes of the Credit Institutions Act.

§ 7. Trust and company service provider

A provider of trust and company services is a natural or legal person who in their economic or professional activities provides a third party with no less than one of following services:

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

- 1) foundation of a company or another legal person;
- 2) acting as a director or management board member in a company, as a partner in a general partnership or in such a position in another legal person, as well as arrangement of assumption of this position by another person;
- 3) enabling use of the address of the seat or place of business, including granting the right to use the address as part of one's contact information or for receiving mail as well as providing companies or other legal persons, civil law partnerships or other similar contractual legal arrangements with services relating to the aforementioned;
- 4) acting as a representative of a civil law partnership or another similar contractual legal arrangement or appointing another person to the position;
- 5) acting as a representative of a shareholder of a public limited company or arrangement of representation of a shareholder by another person, except in the event of companies whose securities have been listed in a regulated securities market and with respect to whom disclosure requirements complying with European Community legislation or equal international standards are applied.

§ 8. Beneficial owner

(1) A beneficial owner is a natural person who, taking advantage of their influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(1¹) A beneficial owner is also a natural person who ultimately holds the shares or voting rights in a company or exercises final control over management of a company in at least one of the following ways:

1) by holding over 25 per cent of shares or voting rights through direct or indirect shareholding or control, including in the form of bearer shares;

2) otherwise exercising control over management of a legal person.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(2) A beneficial owner is also a natural person who, to the extent of no less than 25 per cent determined beforehand, is a beneficiary of a legal person or civil law partnership or another contractual legal arrangement, which administers or distributes property, or who exercises control over the property of a legal person, civil law partnership or another contractual legal arrangement to the extent of no less than 25 per cent.

(3) A beneficial owner is also a natural person who, to an extent not determined beforehand, is a beneficiary of a legal person or civil law partnership or another contractual legal arrangement, which administers or distributes property, and primarily in whose interests a legal person, civil law partnership or another contractual legal arrangement is set up or operates.

(4) Clause 1) of subsection (1¹) of this section does not apply to companies whose securities have been listed on a regulated stock exchange.

[RT I, 29.06.2011, 1 – entry into force 09.07.2011]

§ 9. Property

For the purposes of this Act, property means any object as well as a document certifying the right of ownership of such object or other rights related to the object, including an electronic document, and a benefit received from the object.

§ 10. Obligated person

An obligated person is a person specified in subsection 3 (1) or (2).

§ 11. Business relationship

(1) For the purposes of this Act, 'business relationship' means a relationship of an obligated person, which:

1) in economic or professional activities is established upon entry into a contract for an indefinite period;

2) is not based on a continuing contract, but which may reasonably be expected to last for a certain term and during which the obligated person repeatedly makes independent transactions in the framework of their economic or professional activities, while providing a service or a professional service, performing professional operations or offering goods.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(2) For the purposes of this Act, 'customer' means a person who has a business relationship with an obligated person.

Chapter 2

DUE DILIGENCE

Division 1 Due Diligence Measures

§ 12. Obligation to take due diligence measures

(1) In economic or professional activities an obligated person pays special attention to the activities of a person participating in a transaction or professional operation or of a person using a professional service or of a customer and to circumstances that refer to money laundering or terrorist financing or the connection of which with money laundering or terrorist financing is probable, including to complex, high-value and unusual transactions which do not have any reasonable economic purpose.
[RT I 2009, 27, 164 – entry into force 08.06.2009]

(2) An obligated person takes due diligence measures at least:

- 1) upon establishment of a business relationship;
- 2) upon carrying out or mediating, on an occasional basis, transactions the value of which exceeds 15 000 euros or an equal amount in another currency, regardless of whether the financial obligation is performed in the transaction in a single payment or in several linked payments, unless otherwise provided by law;
[RT I 2010, 22, 108 – entry into force 01.01.2011]
- 3) upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits provided by law;
- 4) when the documents or data gathered earlier while identifying and verifying a person or while updating the respective data prove to be deficient or there is doubt about the veracity of the documents or data.

§ 13. Due diligence measures

(1) To perform the obligation provided in § 12, an obligated person takes the following due diligence measures in economic or professional activities:

- 1) identification of the customer or the person participating in the transaction on the basis of documents and data submitted by him or her and verification of the submitted information on the basis of information obtained from a reliable and independent source;
- 2) identification and verification of the representative of the natural person or of the legal person and the right of representation;
- 3) identification of the beneficial owner, including gathering information about the ownership and control structure of the legal person, trust, civil law partnership or other contractual legal arrangement on the basis of information provided in pre-contractual negotiations or obtained from another reliable and independent source;
- 4) obtaining information on the purpose and nature of the business relationship and transaction;
- 5) constant monitoring of the business relationship, including monitoring transactions carried out during the business relationship, regular verification of data used for identification, updating relevant documents, data or information and, if necessary, identification of the source and origin of funds used in the transaction.

(2) Credit institutions and financial institutions take due diligence measures in an agency, branch or subsidiary where they have a majority shareholding and which is located in a third country and follow there such requirements for collection and keeping of records, which are at least equal to the provisions of this Act. If the legislation of a third country does not allow for taking equal measures, the credit institution or financial institution must immediately notify the competent supervision authority thereof and take additional measures for prevention of money laundering or terrorist financing risks.

§ 14. General taking of due diligence measures

(1) An obligated person takes the due diligence measures provided in clauses 13 (1) 1) to 4) before establishment of any business relationship or carrying out any transaction, unless otherwise provided by this Act.

(2) If a financial obligation is performed in a transaction in several linked payments and the total amount of these payments is unknown, the person must be identified and verified as soon as the exceeding of the amount provided for in clause 12 (2) 2) becomes evident.

(3) An obligated person takes any and all due diligence measures specified in subsection 13 (1) of this Act, but may choose the appropriate scope of taking of the due diligence measures based on the nature of the business relationship or transaction or the risk level of the person participating in the transaction or professional operation, the person using a professional service or the customer.
[RT I 2009, 27, 164 – entry into force 08.06.2009]

(4) Upon taking the due diligence measures specified in clauses 13 (1) 1) #3), an obligated person has the right to rely on information received by the obligated person in a form reproducible in writing from a credit institution registered in the Estonian commercial register or from the branch of a foreign credit institution or from a credit institution that has been registered or whose place of business is in a contracting state of the European Economic Area or a third country where requirements equal to those provided in this Act are in force.

(5) In their economic or professional activities an obligated person pays special attention to business relations and transactions if the place of residence or seat of the customer or the person participating in transaction or the person using the professional service or the seat of the provider of the payment service of the beneficiary is in a third country or in a territory where sufficient measures for preventing money laundering and terrorist financing have not been taken or if the country or territory is not engaged in international cooperation for prevention of money laundering and terrorist financing or if it is a low tax rate territory.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

§ 15. Specifications for taking due diligence measures by credit institutions and financial institutions

(1) Upon opening an account in a credit institution or a financial institution or upon the first use of another service by a person with whom a credit institution or a financial institution has no business relationship, the person participating in the transaction or using the service must be identified while being present at the same place as the person or the person's representative.

(1¹) Identification of a person and verification of the identity of a person using information technology means in accordance with the procedure established on the basis of subsection (1²) of this section is deemed equivalent to the identification of a person and verification of the identity of a person while being present at the same place as the person or their representative, provided that all the following criteria are met:

1) to identify the person and verify the person's identity, a document issued by the Republic of Estonia for the purpose of digital identification is used and, if the person is a foreign national, the identity document issued by the competent authority of the foreign country is also used simultaneously;

2) to identify the person and verify the person's identity, the identification data entered in the identity documents database specified in the Identity Documents Act is used;

3) the credit institution and the financial institution take enhanced due diligence measures in accordance with subsection 19 (3¹) and clauses 21 (2) 1), 3) and 4) of this Act;

4) the establishment of a business relationship with an e-resident is decided by the management board of the credit institution or financial institution or a person or persons authorised by the management board.

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(1²) The requirements of and procedure for identification of persons and verification of persons' identity using information technology means will be established by a regulation of the minister responsible for the field.

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(1³) The regulation specified in subsection (1²) of this section sets out at least requirements for disclosure of information, rules of procedure applicable to the establishment of a business relationship and to the making of a transaction, requirements for activities related to the declarations of intent of the parties to a transaction, organisation of questionnaire surveys and mandatory real-time interviews held upon establishment of a business relationship, conditions of processing of the facial image of a person, and requirements for the quality of the synchronised audio and video stream during the aforementioned procedures as well as for recording and for the reproducibility of recordings.

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(2) A credit institution and a financial institution must not provide services that can be used without identification of the person participating in the transaction and verification of submitted information. A credit institution and a financial institution are also required to open an account and keep an account only in the name of the account holder.

(3) A credit institution and a financial institution must not conclude a contract or make a decision on opening an anonymous account or savings bank book. A transaction in violation of the prohibition is void.

(4) A credit institution and a financial institution may exceptionally, at the request of a person participating in a transaction, open an account before the full taking of due diligence measures on the condition that the account is debited after the full taking of the due diligence measures specified in clauses 13 (1) 1) to 4) and the first payment relating to the transaction is made through an account of the same person, which has been opened in a credit institution that operates in a contracting state of the European Economic Area or in a country where requirements equal to those provided for in this Act are in force.

(4¹) In accordance with the procedure established on the basis of clause 67 (4) 1) of the Commercial Code, a credit institution can, on the basis of personal data automatically checked by the registrar via the computer network or via a notary authorised on the basis of subsection 520 (4) of the Commercial Code, open an account for a company that is being founded, provided that a contribution to the share capital is made to the account via an account opened in a credit institution operating in a contracting state of the European Economic Area or in the branch of a foreign credit institution established in a contracting state of the European Economic Area and the account is not debited before the company has been registered in the Estonian commercial register and

before the due diligence measures specified in clauses 13 (1) 1) to 4) of this Act have been taken in accordance with the procedure set out in subsections (1) and (1¹) of this Act. The representatives of the company must allow the credit institution to take due diligence measures in accordance with the procedure set out in subsections (1) and (1¹) of this section and conclude a payment settlement agreement regarding the account within six months after opening the account.

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(4²) The application of subsection (1) of this section is not mandatory if:

1) the person who wishes to establish a business relationship with a credit institution or a financial institution is a credit institution, insurer, management company, an investment fund established as a legal person or an investment firm who has been granted an authorisation or another equal licence for the provision of a financial service in a contracting state of the European Economic Area or a third country, which is subject to requirements equal to those provided for in this Act and the adherence thereto is subject to state supervision;

2) a credit institution or a financial institution establishes a correspondence relationship established in § 22 of this Act, or

3) a person who wishes to establish a business relationship with a credit institution or a financial institution has been identified and verified by a credit institution or a financial institution specified in subsection (1) of this section, and upon identifying the person, the credit institution or financial institution relies on written information and documents which it has received from a credit institution or financial institution specified in subsection (1) of this section.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(4³) A credit institution or a financial institution that is supervised by the Financial Supervision Authority may, upon opening an account or if another service is used for the first time by a natural person with whom the credit institution or the financial institution does not have a business relationship, identify the person participating in the transaction or using the service without being present in the same place on the basis of a document issued by the Republic of Estonia for digital identification if:

1) the payment transaction relating to the transaction or provision of the service comprises the transfer of money within Estonia and the total amount per calendar month does not exceed 2000 euros until the taking of the due diligence measures specified in clauses 13 (1) 1) to 4) of this Act in accordance with the procedure provided for in subsection (1) of this Act, and

2) until the taking of the due diligence measures specified in clauses 13 (1) 1) to 4) of this Act, the credit institution or the financial institution must not provide third parties with authorisation or authentication services with regard to the person specified in this subsection in accordance with the procedure provided for in subsection (1) of this section.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(4⁴) A credit institution and a financial institution has the right to refuse to provide a payment service or another service and render services to a limited extent to a person who has been identified and whose identity has been verified in accordance with the procedure set out in subsection (1¹) of this section.

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(4⁵) The total amount of the payment orders given to a credit institution or financial institution by a person who has been identified and whose identity has been verified in accordance with the procedure set out in subsection (1¹) of this section must not exceed 10 000 euros per calendar month in the case of a natural person and 25 000 euros per calendar month in the case of a legal person.

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(4⁶) Thresholds lower than the ones specified in subsection (4⁵) of this section or other risk-based restrictions on the execution of payment orders or provision of services by a credit institution or a financial institution to a person who has been identified and whose identity has been verified in accordance with the procedure set out in subsection (1¹) of this section may be established by a regulation of the minister responsible for the field.

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(4⁷) Upon authenticating and authorising a transaction of a customer who has been identified and whose identity has been verified in accordance with the procedure set out in subsection (1¹) of this section on the basis of the e-resident's digital identity card, a credit institution and a financial institution can use only the e-resident's digital identity card.

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(5) An insurer and an insurance broker may verify the identity of a beneficiary under a life assurance contract after the establishment of a business relationship, but not later than upon making a disbursement or commencement of realisation of the rights of the beneficiary arising from the life assurance contract.

(6) Upon provision of currency exchange services, a provider of currency exchange services must identify and verify all persons participating in the transaction if the amounts exchanged in cash either in a single transaction or linked transactions exceed 6400 euros or an equal amount in another currency.

[RT I 2010, 22, 108 – entry into force 01.01.2011]

(7) Upon provision and mediation of a service, a provider of payment services must identify all customers who make or receive money transfers through the provider of payment services.

(8) A provider of services of alternative means of payment must:

1) identify each customer upon establishment of a business relationship and upon making a transaction if the value of the transactions of the customer per calendar month exceeds 1000 euros or an equal sum in another currency;

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

2) upon mediation of a transaction between several customers, identify and verify each person participating in a transaction.

§ 16. Specifications for taking due diligence measures by other obligated persons

(1) An organiser of games of chance must identify and verify the data specified in subsection 23 (3) regarding all persons who pay or receive in a single transaction or several linked transactions an amount exceeding 2000 euros or an equal amount in another currency.

[RT I 2010, 22, 108 – entry into force 01.01.2011]

(2) Identification of persons and the taking of other due diligence measures by a notary is based on the Notarisation Act and the Notaries Act with the specifications provided by this Act.

(3) A notary, enforcement officer, bankruptcy trustee, auditor, attorney and another legal service provider may identify and verify the identity of a customer or a person participating in a transaction and a beneficial owner in the course of establishing a business relationship or carrying out a transaction, provided that it is necessary for the purpose of not interrupting the ordinary course of professional activities and if the risk of financing money laundering or terrorist financing is low.

(4) In the event specified in subsection (3), the taking of due diligence measures must be completed as soon as possible after the first contact and before performing any binding acts.

§ 17. Taking simplified due diligence measures

(1) Upon fulfilment of the conditions provided for in § 18 of this Act, an obligated person may, in the event of a low risk of money laundering or terrorist financing, take the due diligence measures specified in subsection 13 (1) of this Act in accordance with a simplified procedure, determining the appropriate scope thereof in accordance with the nature of the business relationship or the risk level of the risk level of the transaction and the person participating in the transaction or professional operation, person using the professional operation or the customer.

[RT I 2009, 27, 164 – entry into force 08.06.2009]

(2) Simplified due diligence measures are not taken if there is suspicion of money laundering or terrorist financing.

(3) An obligated person must gather enough information to identify whether a transaction performed in economic or professional activities or a person participating in a transaction or professional operation, a person using a professional operation or a customer complies with the conditions provided for in subsections 18 (1)-(4) of this Act.

[RT I 2009, 27, 164 – entry into force 08.06.2009]

§ 18. Conditions of taking simplified due diligence measures

(1) An obligated person may take simplified due diligence measures if a person participating in a transaction carried out in economic or professional activities or participating in a professional operation or a person using a professional service or a customer is:

[RT I 2009, 27, 164 – entry into force 08.06.2009]

1) a legal person governed by public law founded in Estonia;

2) a governmental authority or another authority performing public functions in Estonia or a contracting state of the European Economic Area;

3) an authority of the European Community;

4) a company of a contracting state of the European Economic Area or a third country, which is subject to requirements equal to those provided for in this Act and whose securities are traded in a regulated securities market in one or several contracting state of the European Economic Area;

5) a credit institution or a financial institution, a credit institution or a financial institution located in a contracting state of the European Economic Area or in a third country, which in the country of location is subject to requirements equal to those provided for in this Act and the performance of which is subject to state supervision.

(2) An obligated person may take simplified due diligence measures with regard to the beneficial owners of an official account opened by a notary or enforcement officer of a contracting state of the European Economic Area or third country, provided that the official account is subject to due diligence measures which are in compliance with the international standards for prevention of money laundering and terrorist financing, state supervision is exercised over adherence to these requirements and the notary or enforcement officer has and keeps information about the identity of the beneficial owner.

(3) An insurer or insurance broker may take simplified due diligence measures if:

1) a life assurance contract is made whereby the annual assurance premium does not exceed 1000 euros or a single premium does not exceed 2500 euros;

[RT I 2010, 22, 108 – entry into force 01.01.2011]

2) a pension insurance contract is made which does not provide for the right of withdrawal or cancellation and which cannot be used as loan collateral;

3) a transaction is carried out in the framework of a superannuated pension scheme or another scheme allowing for such pension benefits whereby insurance premium is debited from wages and the terms and conditions of the pension scheme do not allow for assignment of the rights of a participant in the scheme.

(3¹) An electronic money institution may take simplified due diligence measures if an electronic money device does not allow for reloading and the amount saved in one electronic money device does not exceed 250 euros.
[RT I, 08.07.2011, 6 – entry into force 18.07.2011]

(4) An obligated person may take simplified due diligence measures in a transaction if all of the following conditions have been fulfilled:

1) a written contract has been concluded with a customer for an indefinite period;

2) a payment is made through the account of a customer or a person participating in a transaction, which has been opened in a credit institution or the branch of a foreign credit institution registered in the Estonian commercial register or in a credit institution which has been registered or has its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those provided for in this Act are in force;

3) the obligated person has established by rules of internal procedure beforehand that the annual total value of performance of financial obligations arising from transactions of such type does not exceed the maximum limit of 15 000 euros;

[RT I 2010, 22, 108 – entry into force 01.01.2011]

4) the obligated person registers at least the data specified in clauses 23 (2) 1) to 4) of this Act with regard to a customer.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(5) The criteria of the low risk of money laundering or terrorist financing with regard to certain persons or transactions in the event of which simplified due diligence measures may be taken will be established by a regulation of the minister responsible for the field.

§ 19. Taking enhanced due diligence measures

(1) If the nature of a situation involves a high risk of money laundering or terrorist financing, an obligated person must take enhanced due diligence measures.

(2) An obligated person must take the enhanced due diligence measures specified in subsection (3) if:

1) a person participating in a transaction performed in economic or professional activities, a person participating in a professional operation, a person using a professional service or a customer has been identified and verified without being present at the same place as the person or customer;

[RT I 2009, 27, 164 – entry into force 08.06.2009]

2) upon identification or verification of a person suspicion arises regarding the truthfulness of the data or authenticity of the documents submitted or regarding the identification of the beneficial owner or beneficial owners;

3) a person participating in a transaction performed in economic or professional activities, a person participating in a professional operation, a person using a professional service or a customer is a person specified in subsection 21 (1) of this Act.

[RT I 2009, 27, 164 – entry into force 08.06.2009]

(3) In the events specified in subsections (1) and (2) of this section, an obligated person must, in addition to the due diligence measures specified in clauses 13 (1) 1) to 4) of this Act, take at least one of the following enhanced due diligence measures:

[RT I 2009, 61, 401 – entry into force 26.12.2009]

1) identification and verification of a person on the basis of additional documents, data or information, which originates from a reliable and independent source or from a credit institution or the branch of a credit institution registered in the Estonian commercial register or from a credit institution, which has been registered or has its place of business in a contracting state of the European Economic Area or in a country where requirements

equal to this Act are in force, and if in such credit institution the person has been identified while being present at the same place as the person;

2) taking additional measures for the purpose of verifying the authenticity of documents and the data contained therein, among other things, demanding that they be notarised or officially authenticated or confirmation of the correctness of the data by the credit institution specified in clause 1), which issued the document;

3) making the first payment relating to a transaction through an account opened in the name of a person or customer participating in the transaction in a credit institution which has its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those provided for in this Act are in force.

(3¹) An obligated person must, upon identifying a person and upon verifying a person's identity as specified in subsection 15 (1¹) of this Act, take the enhanced due diligence measures specified in clause 3) of subsection (3) of this section and follow the requirements of the regulation established on the basis of subsection 15 (1²) of this Act.

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(4) In the events specified in subsections (1) and (2) an obligated person must take the due diligence measures specified in clause 13 (1) 5) more frequently than usually.

(5) An obligated person is responsible for the proper taking of due diligence measures.

§ 20. Politically exposed person

(1) A politically exposed person is a natural person who performs or has performed prominent public functions, their family members and close associates. A person who, by the date of entry into a transaction, has not performed any prominent public functions for at least a year, and the family members or close associates of such person are not considered politically exposed persons.

(2) For the purposes of this Act, a person performing prominent public functions is:

1) a head of state, head of government, minister or deputy minister;

[RT I, 29.06.2014, 109 – entry into force 01.07.2014]

2) a member of parliament;

3) a justice of a supreme court, constitutional court or another court the judgments of which can be appealed against only in exceptional circumstances;

4) a member of the supervisory board of a state audit institution or central bank;

5) an ambassador, chargé d'affaires and active serviceman having a military rank that belongs to the sub-type of a general officer or flag officer;

[RT I, 12.03.2015, 1 – entry into force 01.01.2016]

6) a member of a directing, supervisory or administrative body of a state company.

(3) The provisions of clauses (2) 1)-5) include positions in the European Union and in other international organisations.

(4) A family member of a person performing prominent public functions is:

1) his or her spouse;

2) a partner equal to a spouse under the law of the person's country of residence or a person who as of the date of carrying out the transaction had shared the household with the person for no less than a year;

3) his or her children and their spouses or partners within the meaning of clause 2);

4) his or her parent.

(5) A close associate of a person performing prominent public functions is:

1) a natural person who has a close business relationship with a person performing prominent public functions or with whom a person performing prominent public functions is the joint beneficial owner of a legal person or contractual legal arrangement;

2) a person who as a beneficial owner has full ownership of a legal person or contractual legal arrangement, which is known to have been founded for the benefit of the person performing prominent public functions.

§ 21. Transactions with politically exposed persons of other Member States and third countries

(1) Upon establishment of a business relationship with or carrying out a transaction with or performance of a professional operation for or provision of a professional service to a politically exposed person of a contracting state of the European Economic Area or a third country or their family member or close associate, an obligated person takes the enhanced due diligence measures provided for in § 19 of this Act.

[RT I 2009, 27, 164 – entry into force 08.06.2009]

(2) In the event specified in subsection (1), an obligated person also implements the following requirements:

1) apply appropriate risk-based internal procedures for making a decision on establishment of a business relationship or entry into a transaction;

2) the management board of the obligated person or a person or persons authorised by the management board decide the establishment of business relationships;

- 3) upon establishment of a business relationship and entry into a transaction, take appropriate measures for identification of the origin of the money or other property used;
- 4) continuously take the due diligence measures specified in clause 13 (1) 5).

§ 22. Correspondent relationships of credit and financial institutions

(1) A credit institution and a financial institution take enhanced due diligence measures upon opening a correspondent account with a credit institution of a third country and during the period of validity of the respective contract, thereby regularly assessing the following:

- 1) based on public information, the nature of the economic activities and the trustworthiness and reputation of the credit institution of the third country and the effectiveness of supervision exercised over the credit institution;
- 2) the control systems of the credit institution of the third country for prevention of money laundering and terrorist financing.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(2) The contract serving as the basis for opening a correspondent account or the rules of procedure of the credit institution must contain the prohibition to open a correspondent account for a credit institution which corresponds to the condition specified in clause (3) 1), and the obligations of the parties:

- 1) upon taking due diligence measures for prevention of money laundering and terrorist financing, including with regard to a customer having access to a payable-through account or another similar account;
- 2) upon submission, on the basis of a query, of data gathered in the course of identification of customers and verification of submitted information;
- 3) upon keeping records and upon performance of the notification obligation and taking other measures for prevention of money laundering and terrorist financing.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(2¹) Prior consent of the management board of the credit institution or financial institution or the person authorised by the management board is required for opening a correspondent account for a credit institution or a financial institution of a third country or for opening a correspondent account in a third country credit institution or financial institution or for signing the corresponding contract.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(3) Credit institutions and financial institutions are prohibited to open or hold a correspondent account in a credit institution, which meets at least one of the following conditions:

- 1) the actual place of management or business of the credit institution is located outside its country of location and the credit institution is not part of the consolidation group or group of undertakings of a credit institution or financial institution that is subject to sufficient supervision;
- 2) an account for a credit institution corresponding to the characteristics specified in clause 1) has been opened in the credit institution;
- 3) according to international standards or the circumstances provided for in this section, which are to be used as a basis for assessment, deficiencies become evident in the trustworthiness of the executives of the credit institution and in assessment of measures for prevention of money laundering and terrorist financing.

(4) An agreement in violation of the prohibition of opening a correspondent account in a credit institution corresponding to the conditions specified in clauses (3) 1) and 2) is void.

(5) Subsections (3) and (4) apply to correspondent relationships with institutions and undertakings whose principal and permanent activity lies in carrying out transactions resembling those provided for in subsection 6 (1) of the Credit Institutions Act.

Division 2 Collection and Keeping of Records

§ 23. Documents and data serving as basis for identification of natural persons

(1) An obligated person identifies a natural person and verify the person on the basis of a document specified in subsection 2 (2) of the Identity Documents Act or a valid travel document issued in a foreign country or a driving license complying with the conditions provided in subsection 4 (1) of the Identity Documents Act. In addition to an identity document, the representative of a person participating in a transaction submits a document in the required form, certifying the right of representation. A person below 7 years of age may be identified on the basis of a birth certificate specified in § 30 of the Vital Statistics Registration Act.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(2) A copy is made of the page of an identity document submitted for identification which contains the personal data and a photograph. In addition, upon identification and verification of the persons specified in subsection (1), an obligated person registers the following personal data:

- 1) the name and the representative's name;
- 2) the personal identification code or, upon absence of a personal identification code, the date and place of birth;
- 3) the name and number of the document used upon identification of the person and verifying the person's identity, the date of issue of the document, the name of the authority that issued the document, and information on making an electronic query for the purpose of verifying data entered in the identity documents database; [RT I, 06.07.2016, 2 – entry into force 16.07.2016]
- 4) the name of the document used upon identification and verification of the right of representation, and its date of issue and the name of the issuer.

(2¹) A copy specified in subsection (2) of this section does not need to be made if the person to be identified has a valid document specified in subsection 2 (2) of the Identity Documents Act and the person is identified and the person's identity is verified on the basis of the identification data entered in the identity documents database. [RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(3) On the basis of the information received from the person specified in subsection (1), an obligated person registers the address of the place of residence and the profession or area of activity of the person. If a customer or a person participating in a transaction carried out in economic or professional activities is a natural person of a contracting state of the European Economic Area or a third country, the obligated person must register the information about whether the person performs or has performed any prominent public functions or is a close associate or a family member of a person performing prominent public functions.

(4) A person participating in a transaction performed in economic or professional activities, a person participating in a professional operation, a person using a professional service or a customer must, at the request of an obligated person, submit documents and provide relevant information required for taking the due diligence measures specified in subsection 13 (1) of this Act. [RT I 2009, 27, 164 – entry into force 08.06.2009]

(5) A representative of a legal person of a foreign country must, at the request of an obligated person, submit a document certifying his or her powers, which has been notarised or certified in accordance with an equal procedure and legalised or authenticated by a certificate substituting for legalisation (apostille), unless otherwise prescribed by an international agreement.

(6) If the documents or data specified in subsections (1) and (3) cannot be received, documents certified or authenticated by a notary or authenticated officially may be used for verification of the identity of a person.

(7) A person a person participating in a transaction or professional operation performed in economic or professional activities, a person using a professional service or a customer must, at the request of an obligated person, certify the correctness of the submitted information and documents by signature. [RT I 2009, 27, 164 – entry into force 08.06.2009]

§ 24. Documents and data serving as basis for identification of legal persons

(1) An obligated person identifies a legal person and its passive legal capacity and verify the information obtained. Legal persons registered in Estonia and branches of foreign companies registered in Estonia are identified on the basis of an extract of a registry card of the relevant register and foreign legal persons are identified on the basis of an extract of the relevant register or a transcript of the registration certificate or an equal document, which has been issued by a competent authority or body not earlier than six months before submission thereof.

(2) The document submitted for identification must set out at least:

- 1) the business name or name, seat and address of the legal person;
- 2) the registry code or registration number;
- 3) the date of issuance of the document and the name of the agency which issued the document.

(3) On the basis of the documents specified in subsection (1) or, if the aforementioned documents do not contain the respective data, on the basis of the information received from the representative of the legal person participating in the transaction, an obligated person registers the following data:

- 1) the names of the director or the members of the management board or a body substituting for it and their authorisation in representing the legal person;
- 2) the area of activity of the legal person;
- 3) telecommunications numbers;
- 4) the data of the beneficial owners of the legal person.

(4) If an obligated person has information that a politically exposed person of another contracting state of the European Economic Area or a third country may be related to a customer or a person participating in a transaction carried out in economic or professional activities, the circumstances specified in subsection 23 (3) must be registered on the basis of the information received from the representative of the legal person in addition to the data specified in subsection (3).

(5) An extract of the registry card does not have to be submitted if the obligated person has access to the data of the commercial register and the register of non-profit associations and foundations via a computer network.

(6) If the document or data specified in subsections (1) and (3) cannot be received, documents certified or authenticated by a notary or authenticated officially are used for verification of the identity of a person.

§ 25. Registration of transaction data

(1) Upon identification and verification of a person, an obligated person registers the date or period of time of entry into a transaction and a description of the content of the transaction.

(2) A credit institution and a financial institution also registers the following data regarding a transaction:

1) upon opening an account, the account type, number, currency and significant characteristics of the securities or other property;

2) upon the deposit of property, the deposit number and the market value of the property on the date of depositing or a detailed description of the property if the market value of the property cannot be determined;

3) upon renting or using a safe deposit box or a safe in a bank, the number of the safe deposit box or safe;

4) upon making a payment relating to shares, bonds or other securities, the type of the securities, the monetary value of the transaction, the currency and the account number;

5) upon entry into a life assurance contract, the account number debited to the extent of the first premium;

6) upon making a disbursement under a life assurance contract, the account number that was credited to the extent of the amount of disbursement;

7) in the event of a payment mediation service: the data the communication of which is compulsory under Regulation (EC) No. 1781/2006 of the European Parliament and Council on information on the payer accompanying transfers of funds (OJ L 345, 8.12.2006, pp. 1-9);

8) in the event of provision of services of alternative means of payment: the names of the payer and the recipient, the payer's personal identification code, and upon absence thereof, the date and place of birth or a unique feature on the basis of which the payer can be identified;

9) in the event of another transaction: the transaction amount, the currency and the account number.

§ 26. Record keeping

(1) An obligated person must keep the original counterparts or copies of the documents specified in §§ 23 and 24, which serve as the basis for identification and verification of a person, and of the documents serving as the basis for establishment of a business relationship, for no less than five years after termination of the business relationship.

(2) An obligated person must keep on any data medium the documents prepared with regard to a transaction and the documents and data serving as the basis for the notification obligations specified in subsections 32 (1) and (2) for no less than five years after carrying out the transaction or performance of the notification obligation.

(3) An obligated person must keep the documents and data specified in sections (1) and (2) in a manner which allows for a full and immediate reply to enquiries received from the Financial Intelligence Unit or, in accordance with legislation, from other investigative bodies or a court.

(4) If an obligated person makes, for the purposes of identifying a person, a query to a database that is part of the state information system and the use of which is obligatory for the obligated person under the legislation in force, the obligation provided for in subsections (1) and (3) of this section will be deemed complied with if the information about making the electronic query to the corresponding register can be reproduced over a period of five years after the end of the business relationship. The obligated person preserves the data of the document prescribed for the digital identification of a person upon identifying the person and verifying the person's identity in accordance with the procedure set out in subsection 15 (1¹) of this Act, information on making an electronic query to the identity documents database, and the audio and video recording of the procedure of identifying the person and verifying the person's identity at least five years following the termination of the business relationship.

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

Division 3

Management of Risks Relating to Money Laundering and Terrorist Financing

§ 27. Refusal from transaction and termination of business relationship

(1) An obligated person is prohibited to establish a business relationship or to carry out a transaction specified in clause 12 (2) 2) of this Act if a person participating in the transaction or professional operation, a person

using professional services or a customer, regardless of the respective request, does not submit the documents or relevant information required for complying with the due diligence measures specified in clauses 13 (1) 1) to 4) of this Act or if on the basis of the documents submitted the obligated person has reasonable doubt that the situation may constitute money laundering or terrorist financing.
[RT I 2009, 27, 164 – entry into force 08.06.2009]

(1¹) Credit institutions are prohibited to sign a settlement contract if the owner of the account specified in subsection 15 (4¹) of this Act, regardless of the respective request, does not submit the corresponding data and documents required for taking the due diligence measures specified in clauses 13 (1) 1) to 4) of this Act or if the submitted documents make the obligated person suspect money laundering or terrorist financing.
[RT I 2008, 27, 177 – entry into force 10.07.2008]

(2) An obligated person has the right to refuse to carry out a transaction if a person participating in a transaction or professional operation, a person using a professional service or a customer, regardless of the respective request, does not submit the documents or relevant information required for identification of the circumstances specified in clauses 13 (1) 1) to 4) of this Act or data certifying the legal origin of the property constituting the object of the transaction or if the data and documents submitted make the obligated person suspect money laundering or terrorist financing.
[RT I 2009, 27, 164 – entry into force 08.06.2009]

(3) If a person participating in a transaction in economic or professional activities or a customer does not, in spite of a respective request, submit documents required for fulfilling the obligation set out in clauses 13 (1) 1) to 4) of this Act or submit relevant information or, in spite of sending repeated invitations, fails to appear at the seat or place of business of the obligated person for the purpose of verifying the circumstances specified in subsection 13 (1) of this Act, it will be deemed as a fundamental breach of the contract and the obligated person will be obligated to extraordinarily terminate the long-term contract serving as the basis for the business relationship without following any term for advance notification.
[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(3¹) A credit institution and a financial institution has the right to extraordinarily terminate the long-term contract serving as the basis for a business relationship if the issue of the e-resident's digital identity card of the person is refused, its validity is suspended or it is declared invalid on the ground set out in subsection 20⁶(2) or (3) of the Identity Documents Act.
[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(4) In the event of termination of a business relationship based on subsection (3) or (3¹), a credit institution and a financial institution is allowed to transfer the customer's assets only to an account that has been opened in a credit institution or branch of a foreign credit institution registered in the Estonian commercial register or in a credit institution registered or having its place of business in a contracting state of the European Economic Area or in a state where requirements equivalent to the requirements of this Act are in force. Subsection 720 (6) of the Law of Obligations Act does not apply to this subsection.
[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(4¹) Any agreement violating the prohibition provided for in subsection (1¹) of this section is void. The provisions of the first sentence of subsection (4) of this section apply to the account of a company being founded, unless otherwise provided in a precept of the Financial Intelligence Unit issued on the basis of subsection 40 (1) of this Act.
[RT I 2008, 27, 177 – entry into force 10.07.2008]

(5) The provisions of subsections (1) to (3¹) do not apply to notaries, attorneys, enforcement officers, bankruptcy trustees, other legal service providers, auditors or persons providing accounting or tax advice when evaluating the customer's legal position, defending or representing the customer in court proceedings, intra-authority appeal proceedings or other similar proceedings, including advising the customer regarding the initiation or avoidance of proceedings.
[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

(6) An obligated person registers and records in accordance with the procedure laid down in § 26 of this Act:
1) information about the circumstances of refusal to establish a business relationship or carry out a transaction by the obligated person;
2) the circumstances of giving up the establishment of a business relationship or carrying out a transaction on the initiative of the person participating in the transaction or professional operation, the person using a professional service or the customer, provided that the giving up is related to the taking of due diligence measures by the obligated person;

2¹) information according to which it is not possible to take the due diligence measures provided for in clauses 13 (1) 1) to 4) of this Act by information technology means;
[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

3) the circumstances of termination of the business relationship in the events set out in subsections (3) and (3¹) of this section;

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

4) the information serving as the basis for the notification obligation arising from § 32 of this Act.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

§ 28. Outsourcing of activities relating to economic or professional activities of obligated persons

(1) If an obligated person has outsourced an activity to a third party for the purpose of better performance of the obligations related to its economic or professional activities, it will be deemed that the third party knows of any and all requirements arising from this Act. The obligated person who outsourced its activities is liable for infringement of the requirements.

(2) The outsourcing of an activity is permitted only if:

- 1) it does not harm the justified interests of the obligated person or the person participating in the transaction;
- 2) it does not impede the activities of the obligated person or performance of the obligations provided in this Act;
- 3) it does not impede exercising state supervision over an obligated person;
- 4) the third party to whom the activities are outsourced has the required knowledge and skills and it is able to fulfil the requirements provided for in this Act;
- 5) the obligated person has the right and opportunity to check performance of the requirements provided in this Act by the third party;
- 6) it is ensured that the documents and records collected for fulfilment of the requirements arising from this Act are kept in accordance with the procedure provided for in this Act and legislation adopted on the basis thereof.

(3) An obligated person notifies the competent supervision authority about outsourcing its activities.

§ 29. Internal security measures

(1) An obligated person must establish written rules of procedure for taking the due diligence measures provided in this Act, including assessment and management of the risk of money laundering and terrorist financing, collection and keeping of records, and performance of the notification obligation and notification of the management, as well as internal control rules for checking adherence thereto.

(1¹) An obligated person must pay special attention to implementing rules of procedure and internal control rules in the subsidiaries where it has a majority holding, in branches and in representative offices if their seat or place of business is located in a third country which does not implement sufficient measures for prevention of money laundering and terrorist financing or does not participate in international cooperation for prevention of money laundering and terrorist financing or if the country is a low tax rate territory. Obligated persons ensure that, upon implementation of rules of procedure and internal control rules in the subsidiaries where they have a majority holding and in their branches and representative located in a third country, requirements at least equivalent to those provided for in this Act are established.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(2) The management board of a legal person constituting an obligated person, the head of the branch of an obligated person or, upon absence of the former, an obligated person must ensure the provision of regular training in the performance of duties arising from this Act for employees whose duties include establishment of business relationships or carrying out transactions. The training must, among other things, give information about the modern methods of money laundering and terrorist financing and the related risks.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(3) The management board of a credit institution and financial institution and the head of the branch of a foreign credit institution and financial institution registered in the Estonian commercial register appoint a person who acts as the contact person of the Financial Intelligence Unit (hereinafter *compliance officer*). Only a person who has the education, professional suitability, abilities, personal characteristics and experience required for performance of the duties of a compliance officer and impeccable reputation may be appointed as a compliance officer. Before the appointment of a compliance officer and during performance of the compliance officer's duties, the Financial Intelligence Unit has the right to receive information from the compliance officer, their employer and state databases for the purpose of verifying the compliance officer's background and suitability. If a structural unit performs the duties of a compliance officer, the provisions of this subsection apply to each employee of the structural unit.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(3¹) For the purposes of this Act, a person does not have impeccable reputation if, as a result of a background check carried out by the Financial Intelligence Unit, it becomes evident that the person's credibility is under suspicion due to their previous acts or omissions. In such an event the credit institution or financial institution may extraordinarily terminate the compliance officer's employment contract due to the loss of credibility.

[RT I, 08.05.2012, 1 – entry 18.05.2012]

(4) An obligated person who is not a credit institution or financial institution may appoint a compliance officer for performance of the duties related to prevention of money laundering and terrorist financing. If a compliance officer has not been appointed, the duties of a compliance officer are performed by the management board of a legal person, the head of the branch of a foreign company registered in the Estonian commercial register, or a self-employed person.

(5) An employee or a structural unit may perform the functions of the compliance officer. If a structural unit performs the duties of the compliance officer, the head of the respective structural unit is responsible for performance of the given duties. The competent supervision authority is notified of the appointment of the compliance officer.

(6) The obligations provided for in this section do not apply to non-profit associations or foundations.
[RT I, 08.05.2012, 1 – entry 18.05.2012]

§ 30. Requirements for rules of procedure

(1) The rules of procedure established by an obligated person must correspond to the type, scope and complexity of the economic or professional activities of the obligated person and regulate the taking of due diligence measures at least in the events specified in subsection 13(1).

(2) An obligated person must regularly check whether the established rules of procedure are up-to-date and establish new rules of procedure where necessary.

(3) The rules of procedure must:

- 1) describe transactions of a lower risk level and establish the appropriate requirements and procedure for carrying out such transactions;
- 2) describe transactions of a higher risk level, including risks arising from telecommunications, information technology means, computer network and other technological development, and establish the appropriate requirements and procedure for carrying out and monitoring such transactions;
[RT I, 06.07.2016, 2 – entry into force 16.07.2016]
- 3) set out the rules of taking the due diligence measures specified in clause 13 (1) 5);
- 4) set out the requirements and procedure for keeping the documents and records specified in Division 2 of this Chapter;
- 5) set out the requirements and procedure for application of subsection 27 (6) of this Act.
[RT I 2009, 61, 401 – entry into force 26.12.2009]

(4) The rules of procedure must contain instructions for how to effectively and quickly identify whether or not the person is:

- 1) a politically exposed person;
- 2) a person whose place of residence or seat is in a country where no sufficient measures for prevention of money laundering and terrorist financing have been taken;
- 3) a person with regard to whose activities there is prior suspicion that the person may be involved in money laundering or terrorist financing;
- 4) a person with regard to whom international sanctions are imposed;
- 5) a person with whom a transaction is carried out using telecommunications.

(5) The rules of procedure are introduced to all employees of an obligated person whose duties include establishment of business relationships or carrying out transactions.

(6) The detailed requirements for the rules of procedure established by credit institutions and financial institutions, internal audit rules for checking performance thereof, and application thereof will be established by a regulation of the minister responsible for the field.

(7) The obligations provided for in this section do not apply to non-profit associations or foundations.
[RT I, 08.05.2012, 1 – entry 18.05.2012]

§ 31. Compliance officer

(1) The organisational structure of credit institutions and financial institutions must be suitable for performance of the requirements arising from this Act and ensure direct subordination of the compliance officer to the management board of the credit institution or financial institution.

(2) The management board of a credit institution or financial institution and the head of the branch of a foreign credit institution or financial institution registered in the Estonian commercial register ensure that the compliance officer has the competence, means and access to relevant information required for performance of the functions provided for in this Act in all structural units of the credit institution or financial institution.

(3) The functions of the compliance officer are:

- 1) organisation of collecting and analysis of information referring to unusual transactions or transactions suspected of money laundering or terrorist financing in the activities of the obligated person;
- 2) notification of the Financial Intelligence Unit in the event of suspicion of money laundering or terrorist financing;

3) periodic submission of written statements on implementation of the rules of procedure to the management board of the credit institution or financial institution or the head of the branch of the foreign credit institution or financial institution registered in the Estonian commercial register;

4) performance of other obligations, which are related to the fulfilment of the requirements of the Act by the credit institution or financial institution.

(4) The compliance officer has the right to:

1) make proposals to the management board of the credit institution or financial institution or the head of the branch of a foreign credit institution or financial institution registered in the Estonian commercial register for amending or modifying the rules of procedure containing requirements for prevention of money laundering and terrorist financing, or for organising training specified in subsection 29 (2);

2) demand that the structural units of the obligated person eliminate within a reasonable term the deficiencies detected in the implementation of the requirements for prevention of money laundering and terrorist financing.

(5) The obligations provided for in this section do not apply to non-profit associations or foundations.

[RT I, 08.05.2012, 1 – entry 18.05.2012]

Chapter 3

CONDUCT IN EVENT OF SUSPICION OF MONEY LAUNDERING OR TERRORIST FINANCING

§ 32. Notification obligation in event of suspicion of money laundering or terrorist financing

(1) If, upon performance of economic or professional activities or professional operations or provision of professional services, an obligated person identifies an activity or circumstances which might be an indication of money laundering or terrorist financing or an attempt thereof or in the event of which the obligated person has reason to suspect or knows that it is money laundering or terrorist financing, the obligated person must immediately, but not later than within two working days from identifying the act or circumstances or from the rise of the suspicion, notify the Financial Intelligence Unit thereof.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(2) Subsection (1) of this section also applies in the event of the circumstances specified in clauses 27 (6) 1) to 3).

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(3) An obligated person, except a credit institution, immediately, but not later than within two working days of executing the transaction, notifies the Financial Intelligence Unit of any transaction where the financial obligation exceeding 32 000 euros or an equal amount in another currency is performed in cash, regardless of whether the transaction is carried out in a single payment or in several linked payments. A credit institution immediately, but not later than within two working days of executing the transaction, notifies the Financial Intelligence Unit of any currency exchange transaction exceeding 32 000 euros in cash, unless the credit institution has a business relationship with the person participating in the transaction.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(4) Notaries and attorneys are not subject to the notification obligation arising from subsections (1) and (3) when evaluating a customer's legal position, defending or representing the customer in court proceedings, intra-authority appeal proceedings or other similar proceedings, including advising the customer regarding the initiation or avoidance of proceedings, regardless of whether the information has been received before, during or after proceedings.

(5) An obligated person has the right to postpone the transaction or professional operation in the event specified in subsection (1). If the postponement of a transaction may cause considerable harm, the transaction has to be carried out or if it may impede catching the person who possibly committed money laundering or terrorist financing, the transaction or professional operation will be carried out and the Financial Intelligence Unit will be notified thereafter.

[RT I 2009, 27, 164 – entry into force 08.06.2009]

§ 33. Place and form of performance of notification obligation

(1) The information is transmitted to the Financial Intelligence Unit of the contracting state of the European Economic Area in whose territory the obligated person is situated.

(2) A notification is communicated orally, in writing or in a form reproducible in writing. If a notification was communicated orally, it will be repeated the next working day in writing or in a form reproducible in writing.

(3) The data used for identifying and verifying a person or, where necessary, copies of relevant documents may be appended to a notification.

(4) The form for notification to be transmitted to the Financial Intelligence Unit and instructions for the preparation thereof will be established by a regulation of the minister responsible for the field.

§ 34. Confidentiality obligation of notifier

(1) An obligated person, and a structural unit, a member of a directing body and an employee of an obligated person who is a legal person is prohibited to notify a person, the beneficial owner or representative of the person about a notification given to the Financial Intelligence Unit about the person and about precepts made by the Financial Intelligence Unit or initiation of criminal proceedings under § 40 or 41. After a precept made by the Financial Intelligence Unit has been complied with, an obligated person may notify a person that the Financial Intelligence Unit has restricted the use of the person's account or that other restrictions have been imposed.

(2) The provisions of subsection (1) are also applied in the event of provision of information to third parties, unless otherwise provided in this Act.

(3) An obligated person may give information to a third party if:

1) the third party belongs to the same consolidation group or financial conglomerate as the obligated person specified in clauses 3 (1) 1) and 2) of this Act and the undertaking is located in a contracting state of the European Economic Area or third country where requirements equal to those provided in this Act are in force, state supervision is exercised over fulfilment thereof and requirements equal to those in force in Estonia are applied for the purpose of keeping professional secrets and protecting personal data;

2) the third party acts in the same legal person or structure, which has joint owners and a joint management or internal control system, as the obligated person who pursues the profession of a notary, attorney or auditor;

3) the information specified in subsection (1) concerns the same person and the same transaction which is related to several obligated persons and the information is given by a credit institution, financial institution, notary, attorney or auditor to a person operating in the same branch of the economy or profession and located in a contracting state of the European Economic Area or third country where requirements equal to those provided in this Act are in force, state supervision is exercised over fulfilment thereof and requirements equal to those in force in Estonia are applied for the purpose of keeping professional secrets and protecting personal data.

(4) Information exchanged in accordance with subsection (3) may be used solely for the purpose of prevention of money laundering and terrorist financing.

(5) The prohibition provided in subsection (1) is not applied if a notary, attorney or auditor tries to convince a customer to refrain from illegal acts.

§ 35. Relief from liability

(1) An obliged person, its employee, representative or a person who acted in its name is not, upon performance of the obligations arising from this Act, liable for damage arising from failure to carry out a transaction or failure to carry out a transaction by the due date if the damage was caused to the person participating in the transaction made in economic or professional activities in connection with notification of the Financial Intelligence Unit of the suspicion of money laundering or terrorist financing in good faith, or for damage caused to a customer or a person participating in a transaction carried out in economic or professional activities in connection with cancellation of a contract concluded for an indefinite period on the basis provided in subsection 27 (3).

(2) The performance in good faith of the notification obligation arising from § 32 and communication of relevant data by an obligated person is not deemed infringement of the confidentiality requirement provided by law or contract and no liability provided by legislation or contract is imputed with regard to the person who performed the notification obligation for disclosure of the information. An agreement derogating from this provision is void.

(3) Upon issuing to the Financial Intelligence Unit data and documents related to the professional activities of a notary on the basis of a precept issued by the Financial Intelligence Unit on the basis of subsection 41 (1) of this Act, the notary is relieved from the confidentiality requirement prescribed in § 3 of the Notaries Act.
[RT I 2009, 61, 401 – entry into force 26.12.2009]

Chapter 4

FINANCIAL INTELLIGENCE UNIT

§ 36. Financial Intelligence Unit

(1) The Financial Intelligence Unit is an independent structural unit of the Police and Border Guard Board.

(2) The Director General of the Police and Border Guard Board appoints the head of the Financial Intelligence Unit on a proposal of the Deputy Director General in the Field of Intelligence Management and Investigation.

[RT I, 19.03.2015, 2 – entry into force 29.03.2015]

(3) The Police and Border Guard Board provides the Financial Intelligence Unit with sufficient funds for performance of the functions provided by law.

[RT I 2009, 62, 405 – entry into force 01.01.2010]

§ 37. Functions of Financial Intelligence Unit

(1) The functions of the Financial Intelligence Unit are:

- 1) to collect, register, process and analyse information received in accordance with §§ 32 and 33 of this Act. In the course thereof, the significance of the information submitted to the Financial Intelligence Unit for the prevention, identification or investigation of money laundering, criminal offences related thereto and terrorist financing is assessed;
- 2) to inform the persons who submit information to the Financial Intelligence Unit of the use of the information submitted for the purposes specified in clause 1) of this section in order to improve the performance of the notification obligation;
- 3) to trace criminal proceeds and application of the enforcement powers of the state on the bases and within the scope provided by law;
- 4) to supervise the activities of obligated persons in complying with this Act, unless otherwise provided by law;
- 5) to inform the public of prevention and identification of money laundering and terrorist financing, analysing the respective statistics, and preparing and publishing an aggregate overview at least once a year;
- 6) to cooperate with obligated persons and investigative bodies in the prevention of money laundering and terrorist financing;

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

7) to train obligated persons, investigative bodies, prosecutors and judges in matters related to prevention of money laundering and terrorist financing;

8) to organise foreign communication and exchange of information in accordance with § 46;

9) to perform the functions arising from the International Sanctions Act;

[RT I 2010, 26, 129 – entry into force 05.10.2010]

10) to conduct proceedings in matters of misdemeanours provided for in this Act;

11) to process applications for authorisations, to suspend or prohibit economic activities or to suspend or revoke an authorisation in accordance with the procedure set out in the General Part of the Economic Activities Code Act, taking account of the specifics of this Act.

[RT I, 29.06.2014, 1 – entry into force 01.07.2014]

(2) The Financial Intelligence Units analyses and verifies information about suspicions of money laundering or terrorist financing, taking measures for preservation of property where necessary and immediately transmitting materials to the competent authorities upon detection of elements of a criminal offence.

§ 38. Administrative decisions of Financial Intelligence Unit

(1) The Financial Intelligence Unit issues precepts and other administrative decisions in order to perform the functions arising from law.

(2) A precept issued on the basis of subsections 40 (1) and (3) and 41 (1) and (4) of this Act does not set out the factual basis for the issue thereof. The facts on the basis of which a precept is issued are set out in a separate document. The person whose transaction was suspended or the use of whose account or other property was restricted by a precept has the right to examine the document presenting the facts. The Financial Intelligence Unit has the right to deny a request to examine a document if this would impede the prevention of money laundering or terrorist financing or hinder the truth from being ascertained in criminal proceedings.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(3) An administrative decision of the Financial Intelligence Unit is signed by the head or deputy head of the Financial Intelligence Unit or by an official authorised by the head of the Financial Intelligence Unit. Upon signature by an authorised official, the number and date of the document granting the right of signature and the place where the document can be reviewed are indicated next to the signature.

(4) In the event of failure to comply with an administrative decision, the Financial Intelligence Unit may impose a coercive measure in accordance with the procedure provided for in the Substitutive Enforcement and Penalty Payment Act. The upper limit for a penalty payment for failure to comply with an administrative decision is 1300 euros for the first occasion and 6000 euros for each subsequent occasion.

[RT I 2010, 22, 108 – entry into force 01.01.2011]

(5) An appeal against an administrative decision issued or an administrative act performed by the Financial Intelligence Unit is filed with an administrative court.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

§ 39. Guidelines of Financial Intelligence Unit

- (1) The Financial Intelligence Unit has the right to issue advisory guidelines to explain legislation regulating the prevention of money laundering and terrorist financing.
- (2) The Financial Intelligence Unit issues advisory guidelines regarding the characteristics of suspicious transactions.
- (3) The Financial Intelligence Unit issues advisory guidelines regarding the characteristics of terrorist financing. The guidelines are coordinated with the Security Police Board beforehand.
- (4) The guidelines of the Financial Intelligence Unit are published on the website of the Financial Intelligence Unit.

§ 40. Suspension of transaction, restriction of disposal of property and transfer of property to state ownership

(1) In the event of suspicion of money laundering or terrorist financing, the Financial Intelligence Unit may issue a precept to suspend a transaction and to impose restrictions on the disposal of an account or other property constituting the object of the transaction, professional operation or professional service or other assets or property suspected of being associated with money laundering or terrorist financing for up to 30 days as of the delivery of the precept. In the event of property registered in the land register, ship register, Estonian Central Register of Securities, traffic register, construction register or another state register, the Financial Intelligence Unit may, in the event of justified suspicion, restrict the disposal of the property for the purpose of ensuring its preservation for up to 30 days.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(2) Before expiry of the term specified in subsection (1) a transaction may be carried out or the restriction of disposal of an account or other property may be derogated from only upon the written consent of the Financial Intelligence Unit. During the time that restrictions on using an account are in force, the credit institution or financial institution does not execute any orders issued by the account holder for debiting the account.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(3) In addition to the provisions of subsection (1) of this section, the Financial Intelligence Unit may, on the basis of a precept, restrict the use of property for up to 60 days for the purpose of ensuring its preservation if:

[RT I 2009, 61, 401 – entry into force 26.12.2009]

1) during verification of the source of the property in the event that there is a suspicion of money laundering, the owner or possessor of the property fails to submit evidence certifying the legality of the source of the property to the Financial Intelligence Unit within 30 days as of the suspension of the transaction or as of the imposition of restrictions on the use of the account or other assets or property;

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

2) there is suspicion that the property is used for terrorist financing.

(3¹) Property subject to restrictions on use imposed by the Financial Intelligence Unit in accordance with the procedure provided for in this section cannot be seized or transferred in enforcement proceedings or bankruptcy proceedings.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(4) If in the event of suspicion of money laundering the legality of the source of the property is verified before the term specified in subsection (3) of this section expires, the Financial Intelligence Unit is required to revoke the restrictions on the disposal of the property immediately.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(5) After submission of the materials specified in subsection 37 (2) of this Act, the competent authority immediately informs the Financial Intelligence Unit of the seizure of, refusal to seize or release from seizure of assets or property in accordance with the procedure provided for in the Code of Criminal Procedure. If assets or property is seized in accordance with the procedure provided for in the Code of Criminal Procedure, the Financial Intelligence Unit must immediately terminate any restrictions of disposal of the assets or property after a court ruling regarding the seizure of the assets or property has entered into force.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(6) If the owner of assets or property has not been identified, the Financial Intelligence Unit may request that the administrative court grant permission to restrict the disposal of the assets or property until the owner of the assets or property has been identified, including also in the event of termination of the criminal procedure, but not for more than one year. The possessor of the assets or property against whom the restriction of disposal of the assets or property is being decided has the right to give an explanation to the administrative court within the prescribed term.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(7) If the owner of assets or property has not been identified within one year after the establishment of restrictions on the disposal of the assets or property, the Financial Intelligence Unit or the Prosecutor's Office may apply to the administrative court for permission to transfer the assets or property to state ownership.

The administrative court decides the granting of the permission in a court hearing. The assets or property are sold in accordance with the procedure provided for in the Code of Enforcement Procedure and the amount received from the sale is transferred to state revenue. The owner of the property has the right to claim an amount corresponding to the value of the assets or property within three years as of the date of transfer of the assets or property to state revenue.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

§ 41. Requesting additional information

(1) To perform the functions arising from law the Financial Intelligence Unit has the right to receive information from the Financial Supervision Authority and other state and local authorities and, on the basis of precepts, from obligated persons regarding the circumstances, transactions or persons related to suspicion of money laundering or terrorist financing.

(2) The addressee of a precept is required to comply with the precept and to submit the requested information, including any information subject to banking or business secrecy, during the term prescribed in the precept. The information is submitted in writing or in a form reproducible in writing.

(3) In order to prevent money laundering, the Financial Intelligence Unit has the right to obtain relevant information, including information collected by surveillance, from any surveillance agency in accordance with the procedure provided by legislation. If the Financial Intelligence Unit wishes to transmit information collected by surveillance which was submitted by a surveillance agency to other agencies, the Financial Intelligence Unit must obtain written consent from the surveillance agency which submitted the information.

(4) On the basis of a precept the Financial Intelligence Unit has the right to receive information from third parties for identification of circumstances which are of relevance in the prevention of money laundering or terrorist financing, including to receive accounting documents on any data medium from a third party whose connection to the investigated transactions became evident in the course of the inspection or analysis.

(5) This section does not apply to attorneys, except in events where the notification submitted by an attorney to the Financial Intelligence Unit does not meet the established requirements, the required documents are not attached to the notice or the attached documents do meet the requirements.

§ 42. Interbase cross-usage of data

In order to perform the functions arising from law, the Financial Intelligence Unit has the right to make enquiries to and to receive data from state and local government databases and databases maintained by persons in public law, in accordance with the procedure provided by legislation.

§ 43. Restrictions on use of information

(1) Only officials of the Financial Intelligence Unit have access to the information in the Financial Intelligence Unit database and the right to process such information.

(2) In order to prevent or identify money laundering or terrorist financing or criminal offences related thereto and in order to facilitate pre-litigation investigation thereof, the Financial Intelligence Unit is required to transmit significant information, including information subject to tax and banking secrecy to the prosecutor, the investigative body and the courts in connection with court proceedings.

(3) Information registered in the Financial Intelligence Unit is transmitted only to the authority engaged in pre-litigation proceedings, a prosecutor or a court in connection with criminal proceedings on the basis of a written request of the preliminary investigation authority, the Prosecutor's Office or the court or on the initiative of the Financial Intelligence Unit if the information is significant for the prevention, identification or investigation of money laundering, terrorist financing or a criminal offence related thereto. The Financial Intelligence Unit has the right to establish restrictions on the use of the data transmitted on its initiative, which the user of the data must adhere to.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

(4) The Financial Intelligence Unit may notify the Financial Supervision Authority of infringement of the requirements established by this Act by credit institutions and financial institutions or, based on a respective request, submit to the Financial Supervision Authority data registered in the Financial Intelligence Unit if it is necessary for performing the duties specified in the Financial Supervision Authority Act, including for the purpose of contributing to the prevention of abusing the financial sector for criminal purposes.

[RT I, 31.12.2015, 38 – entry into force 10.01.2016]

(5) The Financial Intelligence Unit does not disclose the personal data of a person or a member or employee of the directing body of an obligated person performing the notification obligation.

(6) The procedure for the registration and processing of information collected by the Financial Intelligence Unit will be established by a regulation of the minister responsible for the field.

§ 44. Requirements for officials of Financial Intelligence Unit

(1) Only a person with impeccable reputation, the required experience, abilities and education, and high moral qualities may be appointed as an official of the Financial Intelligence Unit.

(2) Officials of the Financial Intelligence Unit are required to maintain the confidentiality of information made known to them in the course of their official duties, including information subject to banking secrecy, even after the performance of their official duties or the termination of a service relationship connected with the processing or use of the information.

§ 45. Cooperation between Financial Intelligence Unit and Security Police Board

(1) The Financial Intelligence Unit and the Security Police Board cooperate in investigation of transactions suspected of terrorist financing through mutual official assistance and exchange of information.

(2) The Director General of the Security Police Board appoints a contact person who has the right to receive information of any and all notifications of suspicion of terrorist financing equally to the official of the Financial Intelligence Unit and to make proposals for requesting additional information where necessary.

(3) The contact person of the Security Police Board is subject to the provisions of clauses 37 (1) 1), 6) and 7), § 41, subsections 43 (1) to (5) and subsection 44 (2).

(4) The contact person of the Security Police Board has the right to exercise supervision specified in § 48 jointly with the Financial Intelligence Unit.

§ 46. International exchange of information

The Financial Intelligence Unit has the right to exchange information and conclude cooperation agreements with foreign agencies which perform the functions of a financial intelligence unit.

Chapter 5 SUPERVISION

§ 47. Supervisory authorities

(1) The Financial Intelligence Unit exercises state supervision over fulfilment of the requirements arising from this Act and legislation adopted on the basis thereof, unless otherwise provided in this section.
[RT I, 13.03.2014, 4 – entry into force 01.07.2014]

(2) The Financial Supervision Authority exercises supervision over fulfilment by credit institutions and financial institutions which are subject to supervision by the Financial Supervision Authority under the Financial Supervision Authority Act of the requirements arising from this Act and legislation adopted on the basis thereof. The Financial Supervision Authority exercises supervision in accordance with the procedure provided for in the Financial Supervision Authority Act.
[RT I 2009, 61, 401 – entry into force 26.12.2009]

(3) The board of the Estonian Bar Association (hereinafter the Bar Association) exercises supervision over fulfilment of the requirements arising from this Act and legislation adopted on the basis thereof by the members of the Bar Association on the basis of the Bar Association Act, taking into account the provisions of this Chapter.

(4) The Ministry of Justice exercises supervision over fulfilment of the requirements arising from this Act and legislation adopted on the basis thereof by notaries on the basis of the Notaries Act, taking into account the provisions of this Chapter. The Ministry of Justice may delegate supervision to the Chamber of Notaries.

(5) The Financial Supervision Authority, the board of the Bar Association, the Ministry of Justice and the Chamber of Notaries cooperate with the Financial Intelligence Unit in accordance with the goals of this Act.

(6) Supervisory authorities have the right to exchange information and cooperate with the supervisory authorities of other states, taking account of the functions provided for in this Act.
[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

§ 47¹. Special measures of state supervision

(1) A law enforcement authority may, for the purpose of exercising the state supervision provided for in this Act, take special measures of state supervision provided for in §§ 30, 31, 32, 35, 50 and 51 of the Law

Enforcement Act on the grounds and in accordance with the procedure provided for in the Law Enforcement Act.

(2) On the conditions provided for in § 50 of the Law Enforcement Act, a law enforcement authority may enter the seat and the place of business of an obligated person as well as a building and a room that the obligated person possesses only in the presence of the inspected person or its representative.
[RT I, 13.03.2014, 4 – entry into force 01.07.2014]

§ 48. Rights of administrative supervision authority

[RT I, 13.03.2014, 4 – entry into force 01.07.2014]

(1) The administrative supervision authority has the right to inspect the seat or the place of business of obligated persons. The administrative supervision authority has the right to enter a building and a room that the obligated person possesses in the presence of a representative of the inspected person.
[RT I, 13.03.2014, 4 – entry into force 01.07.2014]

(2) In the event of on-site inspection, the administrative supervision authority has the right to:
[RT I, 13.03.2014, 4 – entry into force 01.07.2014]

1) without limitations inspect the required documents and data media, make extracts, transcripts and copies thereof, receive explanations regarding them from the obligated person, and monitor the work processes;
2) receive oral and written explanations from the obligated person being inspected, members of its directing body or employees.

(3) The administrative supervision authority has the right to demand that an obligated person submit information required for inspection also without carrying out an on-site inspection.
[RT I, 13.03.2014, 4 – entry into force 01.07.2014]

§ 49. Obligations of supervision authority

(1) If upon exercising supervision the Financial Supervision Authority, the board of the Bar Association, the Ministry of Justice or the Chamber of Notaries detects a situation the elements of which give rise to justified suspicion of money laundering or terrorist financing, they will immediately notify the Financial Intelligence Unit thereof in accordance with the procedure provided in subsection 33 (4).

(2) The Financial Supervision Authority, the board of the Bar Association and the Ministry of Justice must submit the following information about the previous calendar year to the Financial Intelligence Unit by April 15:

1) the number of supervisory procedures conducted and the number of obligated persons covered by supervision, across the types of the obligated persons;
2) violations detected upon exercising supervision, the number of penalised persons and the legal bases of the penalties, for each obligated person.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

§ 50. Reporting of inspection results

(1) The supervision authority must prepare a report on the inspection results, which is communicated to the inspected person within one week after the inspection.

(2) The inspection report must contain the following data:

1) the name of the inspection operation;
2) the official title and the given name and surname of the author of the inspection report;
3) the place and date of drawing up the inspection report;
4) reference to provisions serving as the basis for the inspection;
5) the given name and surname and the official title of the representative of the inspected person or the representative of the possessor of the building or room who attended the inspection;
6) the given name and surname and the official title of another person who attended the inspection;
7) the time of the beginning and end of the inspection and the conditions of the inspection;
8) the process and results of the inspection with the required level of detail.

(3) The author of the inspection report signs it. The inspection report remains with the supervisory official and a copy thereof remains with the inspected person or its representative.

(4) The inspected person has the right to submit written explanations within seven days after the receipt of the inspection report.

[RT I, 13.03.2014, 4 – entry into force 01.07.2014]

§ 51. Supervision over activities of Financial Intelligence Unit

(1) The Data Protection Inspectorate exercises supervision over the legality of the processing of information registered in the Financial Intelligence Unit.

(2) The Police and Border Guard Board exercises supervision over the legality of the activities of the Financial Intelligence Unit.

(3) The Director General of the Police and Border Guard Board and an official authorised by the Director General has the right to access information registered in the Financial Intelligence Unit to the extent required for exercising supervision.

(4) The restriction provided for in subsection 43 (5) and the obligation provided for subsection 44 (2) of this Act apply to an official exercising supervision.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

Chapter 6 AUTHORISATION

[RT I, 29.06.2014, 1 - entry into force 01.07.2014]

§ 52. Authorisation obligation

(1) An undertaking is required to have authorisation for operating in the following areas of activity:

- 1) operating as a financial institution;
- 2) providing trust and company services;
- 3) providing currency exchange services;
- 4) providing services of alternative means of payment;
- 5) providing pawnbroking services;
- 6) buying-in or wholesale of precious metals, precious metal articles or precious stones, except precious metals and precious metal articles used for production, scientific or medical purposes.

(2) The authorisation obligation does not apply to a person who holds:

- 1) an authorisation granted by the Financial Supervision Authority or
- 2) an authorisation granted by the financial supervision authority of a contracting state based on which the person is authorised to operate in Estonia via a branch or across borders, provided that the Financial Supervision Authority has been notified of such operations.

[RT I, 11.03.2016, 1 – entry into force 21.03.2016]

(3) In addition to the information required in the General Part of the Economic Activities Code Act, an application for authorisation must contain the following data and documents:

- 1) the address of the place of provision of the service, including the website address;
- 2) the name and contact details of the person in charge of provision of the service with regard to all the places of provision of the service specified in clause 1) of this subsection;
- 3) the name, personal identification code (upon absence thereof, the date of birth), place of birth and the address of the place of residence of the beneficial owner of the undertaking who is a legal person;
- 4) if the undertaking who is a legal person has not been registered in the Estonian commercial register, the authorisation application must contain the name, registry code or personal identification code (upon absence thereof, the date of birth), place of birth and place of residence of the owner of the undertaking who is a legal person;
- 5) the name, personal identification code or, upon absence thereof, the date and place of birth and the address of the place of residence of a member of the directing body or a procurator of the service provider who is a legal person, unless the service provider is an undertaking registered in the Estonian commercial register;
- 6) the rules of procedure and internal audit rules drawn up in accordance with §§ 29 and 30 of this Act and, in the event of persons having specific obligations listed in § 6 of International Sanctions Act, the rules of procedure and the procedure for verifying adherence thereto drawn up in accordance with subsection 13 (6) of the International Sanctions Act;
- 7) the name, personal identification code (upon absence thereof, the date of birth), place of birth, citizenship, the address of the place of residence, position and contact details of the compliance officer specified in subsection 29 (3) or 29 (4) of this Act,
- 8) the name, personal identification code (upon absence thereof, the date of birth), place of birth, citizenship, the address of the place of residence, position and contact details of the person who is in charge of the imposition of the international financial sanction and who has been appointed by the undertaking in accordance with subsection 13 (6) of the International Sanctions Act;
- 9) if the undertaking, a member of its management body, procurator, beneficial owner or owner is a foreign national or if the undertaking is a foreign service provider, a certificate of the register of convictions or an equal document issued by a competent judicial or administrative body of its country of origin, which certifies the absence of a penalty for an offence against the authority of the state or a money laundering offence or another wilfully committed criminal offence and has been issued no more than three months ago and has been notarised or authenticated and legalised in accordance with an equivalent procedure or authenticated with a certificate replacing legalisation (apostille), unless otherwise provided by an international agreement.

[RT I, 19.03.2015, 4 – entry into force 29.03.2015]

(4) If an undertaking would like to use the authorisation in the activities of its subsidiary, the undertaking must, in addition to the information required in the General Part of the Economic Activities Code Act, submit all the information regarding the subsidiary, which is specified in subsection 52 (3) of this Act.

[RT I, 29.06.2014, 1 – entry into force 01.07.2014]

§ 52¹. Applying for authorisation

An application for authorisation is processed by the Financial Intelligence Unit, an independent structural unit of the Police and Border Guard Board, by granting or refusing to grant the authorisation within 30 working days as of the date of submission of the application.

[RT I, 29.06.2014, 1 – entry into force 01.07.2014]

§ 52². Object of inspection of authorisation

Authorisation will be granted to an undertaking if:

- 1) the undertaking, a member of its management body, procurator, beneficial owner and owner does not have any unexpired penalty for a criminal offence against the authority of the state, criminal offence relating to money laundering or another wilfully committed criminal offence;
- 2) the compliance officer appointed by the undertaking on the basis of subsection 29 (3) of this Act complies with the requirements provided by law;
- 3) the undertaking's subsidiary for whose activities the authorisation to be applied in the name of the undertaking is to be used complies with the requirements specified in clauses 1) and 2) of § 52² of this Act.

[RT I, 29.06.2014, 1 – entry into force 01.07.2014]

§ 52³. Obligation to enclose documents with notice of intention to change economic activities

If an undertaking submits a notice of intention to change the economic activities regarding a change of the undertaking, a member of its management body, procurator, beneficial owner or owner, the document specified in clause 52 (3) 9) of this Act must be enclosed with the notice if the undertaking is a foreign service provider or the member of its management body, procurator, beneficial owner or owner is a foreign national.

[RT I, 29.06.2014, 1 – entry into force 01.07.2014]

§ 52⁴. Obligation to notify of change of circumstances relating to economic activities

In a notice of the intention to change the economic activities and in a notice of the change of economic activities the undertaking must describe which circumstances that form a part of the object of inspection of the authorisation or relate to the secondary conditions of the authorisation have changed or are to be changed or the undertaking must submit, regarding its undertaking that will commence economic activities within the object of regulation of the authorisation, all the information specified in subsection 3) of § 52 of this Act regarding the subsidiary and the information specified in clauses 15 (1) 1)-3) and 5) and 6) of the General Part of the Economic Activities Code Act.

[RT I, 29.06.2014, 1 – entry into force 01.07.2014]

§ 52⁵. Revocation of authorisation

In addition to the grounds provided for in subsection 37 (1) of the General Part of the Economic Activities Code Act, the Financial Intelligence Unit as an independent structural unit of the Police and Border Guard Board will revoke an authorisation specified in subsection 52 (1) of this Act if the Financial Supervision Authority has granted authorisation to the undertaking.

[RT I, 19.03.2015, 4 – entry into force 29.03.2015]

§ 53.–§ 56.[Repealed – RT I, 29.06.2014, 1 – entry into force 01.07.2014]

Chapter 7 LIABILITY

§ 57. Violation of identification obligation

(1) The penalty for violation of the identification and verification obligation provided for in this Act by an obligated person or a member of a management body or an employee thereof is a fine of up to 300 fine units or detention.

[RT I, 12.07.2014, 1 – entry into force 01.01.2015]

(2) The penalty for the same act committed by a legal person is a fine of up to 32 000 euros.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 57¹. Violation of requirements for collecting information

(1) The penalty for violation of requirements for collecting information on the purpose and nature of a business relationship or transaction by an obligated person or a member of a management body or an employee thereof is a fine of up to 300 fine units.
[RT I, 12.07.2014, 1 – entry into force 01.01.2015]

(2) The penalty for the act specified in subsection (1) of this section, if committed by a legal person, is a fine of up to 32 000 euros.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 57². Violation of requirements for taking enhanced due diligence measures

(1) The penalty for violation of requirements for taking enhanced due diligence measures or failure to take enhanced due diligence measures, including violation of requirements for carrying out transactions with politically exposed persons of a third country, on the part of an obligated person or an employee thereof is a fine of up to 200 fine units.
[RT I 2009, 61, 401 – entry into force 26.12.2009]

(2) The penalty for the act specified in subsection (1) of this section, if committed by a legal person, is a fine of up to 20 000 euros.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 57³. Opening anonymous account or savings book

(1) The penalty for making a decision to open an anonymous account or savings book or signing a corresponding contract on the part of an employee of a credit or financial institution is a fine of up to 300 fine units.
[RT I 2009, 61, 401 – entry into force 26.12.2009]

(2) The penalty for the act specified in subsection (1) of this section, if committed by a legal person, is a fine of up to 32 000 euros.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 58. Violation of requirement to register information and keep records

(1) The penalty for violation of the requirement to register information and keep records as provided for in this Act is a fine of up to 300 fine units.

(2) The penalty for the same act committed by a legal person is a fine of up to 32 000 euros.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 59. Failure to submit and late submission of mandatory information

The penalty for failure on the part of an employee of an obligated person to submit mandatory information provided for in this Act to the compliance officer or the manager, or wilful failure to submit such mandatory information on time, is a fine of up to 300 fine units.

§ 59¹. Violation of requirement to constantly monitor business relationships

(1) The penalty for violation of requirement to constantly monitor business relationships as provided for in this Act on the part of an obligated person or an employee thereof is a fine of up to 200 fine units.

(2) The penalty for the act specified in subsection (1) of this section, if committed by a legal person, is a fine of up to 20 000 euros.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 60. Violation of obligation to report suspicion of money laundering or terrorist financing

[RT I, 12.07.2014, 1 – entry into force 01.01.2015]

(1) The penalty for violation of the obligation to notify the Financial Intelligence Unit of a suspicion of money laundering or terrorist financing, a currency exchange transaction or another transaction whereby a financial obligation exceeding 32 000 euros or an equal amount in another currency is performed in cash is a fine of up to 300 fine units or detention.
[RT I, 12.07.2014, 1 – entry into force 01.01.2015]

(2) The penalty for the same act committed by a legal person is a fine of up to 32 000 euros.

[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 61. Unlawful notification of information submitted to Financial Intelligence Unit

(1) The penalty for unlawful notification of a person or the beneficial owner of a person by the manager, compliance officer or another employee of an obligated person or by an employee of a supervision authority about a notification or data submitted to the Financial Intelligence Unit regarding the person or the precepts made by the Financial Intelligence Unit or criminal proceedings instituted regarding the person is a fine of up to 300 fine units or detention.

(2) The penalty for the same act committed by a legal person is a fine of up to 32 000 euros.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 62. Failure to take internal security measures

(1) The penalty for failure by the manager of an obligated person to establish rules of procedure for taking due diligence measures, assessment and management of the risk of money laundering and terrorist financing, collection of information, record keeping and performance of the notification obligation and failure by the manager of a credit institution or a financial institution to appoint a compliance officer is a fine of up to 300 fine units.

(2) The penalty for the same act committed by a legal person is a fine of up to 32 000 euros.
[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 62¹. Violation of requirements for correspondent banking

(1) The penalty for violation of requirements for establishing correspondent relations with a credit or financial institution of a third country as provided for in this Act, on the part of an employee of a credit or financial institution is a fine of up to 200 fine units.

[RT I 2009, 61, 401 – entry into force 26.12.2009]

(2) The penalty for the act specified in subsection (1) of this section, if committed by a legal person, is a fine of up to 20 000 euros.

[RT I 2010, 22, 108 – entry into force 01.01.2011]

§ 63. Violation of obligations of providers of payment services

[Repealed – RT I, 08.07.2011, 6 – entry into force 18.07.2011]

§ 64. Violation of registration obligation

[Repealed – RT I, 29.06.2014, 1 – entry into force 01.07.2014]

§ 64¹. Violation of obligation to notify of change of circumstances relating to economic activities

The penalty for failure to notify of the intention to change the circumstances relating to the object of inspection or the secondary conditions of the authorisation granted to a financial institution not subject to supervision by the Financial Supervision Authority or to a provider of trust and company services or to a provider of currency exchange services or to a provider of services of alternative means of payment or to a pawnbroker or to a person engaged in buying-in or wholesale of precious metals, precious metal articles or precious stones (except precious metals and precious metal articles used for production, scientific or medical purposes) or violation of the obligation to notify of the termination of the activities of a service provider is a fine of up to 32 000 euros.

§ 65. Proceedings

(1) [Repealed – RT I, 12.07.2014, 1 – entry into force 01.01.2015]

(2) Extrajudicial proceedings concerning the misdemeanours specified in §§ 57-64¹ are conducted by the Police and Border Guard Board and the Financial Supervision Authority.
[RT I, 29.06.2014, 1 – entry into force 01.07.2014]

Chapter 8

IMPLEMENTING PROVISIONS

§ 66. Entry into force of registration obligation of pawnbrokers, trust and company service providers and financial institutions

Chapter 6 of this Act will enter into force with regard to pawnbrokers, trust and company service providers and financial institutions not subject to supervision exercised by the Financial Supervision Authority on 15 June 2008.

§ 66¹. Registration obligation of person engaged in the buying-in or wholesale of precious metals, precious metal articles or precious stones, except precious metals and precious metal articles used for production, scientific or medical purposes

A person engaged in the buying-in or wholesale of precious metals, precious metal articles or precious stones, except precious metals and precious metal articles used for production, scientific or medical purposes before entry into force of clause 52 (1) 7) of this Act must bring their activities into compliance with clause 52 (1) 7) of this Act by 1 September 2012.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

§ 66². Implementation of subsection 36 (2) of this Act

The head of the Financial Intelligence Unit who is in office at the time of entry into force of the wording of 18 April 2012 of this Act is considered as appointed to office for five years as of the entry into force of the wording.

[RT I, 08.05.2012, 1 – entry into force 18.05.2012]

§ 66³. Follow-up analysis of wording adopted on 15 June 2016 this year

By 31 December 2017 the Ministry of Finance will analyse the practicality and purposefulness of the mandatory procedural rule of conducting a real-time interview upon establishment of a business relationship, which is set out in the wording adopted on 15 June 2016 and, if necessary, make legislative amendment proposals to the Finance Committee of the *Riigikogu*.

[RT I, 06.07.2016, 2 – entry into force 16.07.2016]

§ 67.–§ 72.[Omitted from this text.]

¹Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ L 309, 25.11.2005, pp. 15-36); Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis (OJ L 214, 04.08.2006, pp. 29-34).