Issuer:	Riigikogu
Type:	act
In force from:	15.03.2019
In force until:	31.12.2019
Translation published:	25.03.2019

Money Laundering and Terrorist Financing Prevention Act[1]

Passed 26.10.2017

Amended by the following acts

Passed	Published	Entry into force
26.10.2017	RT I, 17.11.2017, 2	27.11.2017, partially 01.01.2018
19.12.2018	RT I, 04.01.2019, 12	14.01.2019
20.02.2019	RT I, 13.03.2019, 2	15.03.2019

Chapter 1
GENERAL PROVISIONS

Division 1
Purpose and Scope of Regulation of Act

§ 1. Purpose and scope of regulation of Act

(1) The purpose of this Act is, by increasing the trustworthiness and transparency of the business environment, to prevent the use of the financial system and economic space of the Republic of Estonia for money laundering and terrorist financing.

(2) This Act regulates:
1) the principles of assessment, management and mitigation of risks related to money laundering and terrorist financing;
2) the grounds of the activities of the Financial Intelligence Unit;
3) supervision over obliged entities in complying with this Act;
4) duties and obligations of legal persons in relation to the collection and disclosure of the data of their beneficial owners;
5) duties and obligations related to the collection and disclosure of the data of liability account holders;
6) the liability of obliged entities for a breach of the requirements arising from this Act.

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

§ 2. Application of Act

(1) This Act applies to the economic and professional activities of the following persons: 1) credit institutions;
2) financial institutions;
3) gambling operators, except for organisers of commercial lotteries;
4) persons who mediate transactions involving the acquisition or the right of use of real estate;
5) traders within the meaning of the Trading Act, where a cash payment of no less than 10 000 euros or an equal amount in another currency is made to or by the trader, regardless of whether the financial obligation is performed in the transaction in a lump sum or by way of several linked payments over a period of up to one year, unless otherwise provided by law;
6) persons 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;
7) auditors and providers of accounting services;
8) providers of accounting or tax advice services;

9) providers of trust and company services;
10) providers of a service of exchanging a virtual currency against a fiat currency;
11) providers of a virtual currency wallet service;
12) a central securities depository where it arranges the opening of securities accounts and provides services related to register entries without the mediation of an account operator;
13) undertakings providing a cross-border cash and securities transportation service;
14) pawnbrokers.

(2) This Act applies to the economic or professional activities of notaries, attorneys, enforcement officers, bankruptcy trustees, interim trustees and providers of other legal services where they act in the name and on account of a customer in a financial or real estate transaction. This Act also applies to the economic or professional activities of a said person where the person guides the planning or making of a transaction or makes a professional act or provides a professional service related to:
1) the purchase or sale of an immovable, business or shares of a company;
2) the management of the customer's money, securities or other property;
3) the opening or management of payment accounts, deposit accounts or securities accounts;
4) the acquisition of funds required for the foundation, operation or management of a company;
5) the foundation, operation or management of a trust, company, foundation or legal arrangement.

(3) This Act applies to non-profit associations for the purposes of the Non-profit Associations Act and to other legal persons governed by the provisions of the Non-profit Associations Act as well as to foundations for the purposes of the Foundations Act where they are paid or they pay over 5000 euros in cash or an equal amount in another currency, regardless of whether it is paid in a lump sum or by way of several linked payments over a period of up to one year.

(4) This Act applies to Eesti Pank where it removes from circulation or exchanges banknotes or coins worth of over 10 000 euros or an equal sum in another currency or where it is paid over 10 000 euros in cash or an equal sum in another currency for collector coins or other numismatic-bonistic products, regardless of whether it is paid in a lump sum or in several linked payments over a period of up to one year.

Division 2
Definitions

§ 3. Definitions used in Act

For the purposes of this Act, the following definitions apply:
1) 'cash' means cash within the meaning of Article 2(2) of Regulation (EC) No 1889/2005 of the European Parliament and of the Council on controls of cash entering or leaving the Community (OJ L 309, 25.11.2005, pp 9–12);
2) 'property' means any object as well as the right of ownership of such object or a document certifying the rights related to the object, including an electronic document, and the benefit received from such object;
3) 'obliged entity' means a person specified in § 2 of this Act;
4) 'business relationship' means a relationship that is established upon conclusion of a long-term contract by an obliged entity in economic or professional activities for the purpose of provision of a service or sale of goods or distribution thereof in another manner or that is not based on a long-term contract, but whereby a certain duration could be reasonably expected at the time of establishment of the contact and during which the obliged entity repeatedly makes separate transactions in the course of economic or professional activities while providing a service or professional service, performing professional acts or offering goods;
5) 'customer' means a person who has a business relationship with an obliged entity;
6) 'precious stones' means natural and artificial precious stones and semi-precious stones, their powder and dust, and natural and cultivated pearls;
7) 'precious metal' means precious metal within the meaning of the Precious Metal Articles Act;
8) 'precious metal article' means a precious metal article within the meaning of the Precious Metal Articles Act;
9) 'virtual currency' means a value represented in the digital form, which is digitally transferable, preservable or tradable and which natural persons or legal persons accept as a payment instrument, but that is not the legal tender of any country or funds for the purposes of Article 4(25) of Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, pp. 35–127) or a payment transaction for the purposes of points (k) and (l) of Article 3 of the same Directive;
10) 'virtual currency wallet service' means a service in the framework of which keys are generated for customers or customers' encrypted keys are kept, which can be used for the purpose of keeping, storing and transferring virtual currencies;
11) 'politically exposed person' means a natural person who is or who has been entrusted with prominent public functions including a head of State, head of government, minister and deputy or assistant minister; a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors or of the board of a central bank; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or

supervisory body of a State-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials;
12) 'local politically exposed person' means a person specified in clause 11 of this section who is or who has been entrusted with prominent public functions in Estonia, another contracting state of the European Economic Area or an institution of the European Union;
13) 'family member' means the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or local politically exposed person; a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or local politically exposed person; a parent of a politically exposed person or local politically exposed person;
14) 'person known to be close associate' means a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person or a local politically exposed person; and a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person or local politically exposed person;
15) 'senior management of obliged entity' means an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the management board;
16) 'foreign exchange services' means the exchanging of a valid currency against another valid currency by an undertaking in its economic or professional activities;
17) 'group' means a group of undertakings which consists of a parent undertaking, its subsidiaries within the meaning of § 6 of the Commercial Code, and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings that constitute a consolidation group for the purposes of subsection 3 of § 27 of the Accounting Act;
18) 'high-risk third country' means a country specified in a delegated act adopted on the basis of Article 9(2) of Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141/73, 05.06.2015, pp 73–117).

§ 4. Money laundering

(1) 'Money laundering' means:
1) the conversion or transfer of property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions;
2) the acquisition, possession or use of property derived from criminal activity or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein;
3) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity.

(2) Money laundering also means participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the activities referred to in subsection 1 of this section.

(3) Money laundering is regarded as such also where a criminal activity which generated the property to be laundered was carried out in the territory of another country.

(4) Knowledge, intent or purpose required as an element of the activities referred to in subsections 1–3 of this section may be inferred from objective facts.

(5) Money laundering is regarded as such also where the details of a criminal activity which generated the property to be laundered have not been identified.

§ 5. Terrorist financing

'Terrorist financing' means the financing and supporting of an act of terrorism and commissioning thereof as well as the financing and supporting of travel for the purpose of terrorism within the meaning of §§ $237^{3}$and $237^{6}$of the Penal Code.
[RT I, 04.01.2019, 12 - entry into force 14.01.2019]

§ 6. Credit institution and financial institution

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

1) a credit institution within the meaning of Article 4(1)(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.06.2013, pp 1–337);
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 foreign exchange service provider;
2) a payment service provider within the meaning of the Payment Institutions and E-money Institutions Act, except for a payment initiation service provider and an account information service provider;
3) an e-money institution within the meaning of the Payment Institutions and E-money Institutions Act;
4) an insurance undertaking within the meaning of the Insurance Activities Act (hereinafter *insurance undertaking*) to the extent that it provides services related to life insurance, except for services related to mandatory funded pension insurance contracts within the meaning of the Funded Pensions Act;
5) an insurance broker within the meaning of the Insurance Activities Act (hereinafter *insurance broker*) to the extent that it is engaged in marketing life insurance or provides other instrument-related services;
6) a management company, except upon managing a mandatory pension fund within the meaning of the Funded Pensions Act, and an investment fund founded as a public limited company within the meaning of the Investment Funds Act;
7) an investment firm within the meaning of the Securities Market Act;
8) a creditor and a credit intermediary within the meaning of the Creditors and Credit Intermediaries Act;
9) a savings and loan association within the meaning of the Savings and Loan Associations Act;
10) a central contact point designated by an e-money institution or a payment service provider;
11) another financial institution within the meaning of the Credit Institutions Act;
12) the branch of a foreign service provider registered in the Estonian commercial register providing a service specified in clauses 1–8.

§ 7. Correspondent relationship

For the purposes of this Act, 'correspondent relationship' means:
1) the consistent and long-term provision of banking services by a credit institution (correspondent bank) to another credit institution (respondent bank), including providing a current account, liability account or other account service or other related services such as cash management, international funds transfers, cheque clearing, payable-through accounts and foreign exchange services;
2) the relationships between and among credit institutions and financial institutions, including where similar services are provided by a correspondent bank to a respondent bank for the purpose of servicing its customers, and including relationships established for securities transactions or funds transfers.

§ 8. Provider of trust and company services

For the purposes of this Act, 'provider of trust and company services' means a natural person or a legal person who in its economic or professional activities provides a third party with at least one of the following services:
1) foundation of a company or another legal person, including acts and steps related to the transfer of shareholding;
2) acting as an officer 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 such 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 details or for receiving mail as well as providing a company or another legal person, civil law partnership or a legal arrangement with services relating to the aforementioned;
4) acting as a representative or trustee of a trust, except for a trust within the meaning specified in subsection 2 of § 2 of the Investment Funds Act, or that of a civil law partnership, community or a legal arrangement, or the appointment of another person to such position;
5) acting as a representative of a shareholder of a public limited company or arrangement of the representation of a shareholder by another person, except in the case of companies whose securities have been listed in a regulated securities market and with respect to whom disclosure requirements complying with European Union legislation or equivalent international standards are applied.

§ 9. Beneficial owner

(1) For the purposes of this Act, 'beneficial owner' means a natural person who, taking advantage of their influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favour or on whose account a transaction or act, action, operation or step is made.

(2) In the case of companies, a beneficial owner is the natural person who ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means.

(3) Direct ownership is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company. Indirect ownership is a manner of exercising control whereby a company which is under the control of a natural person holds or

multiple companies which are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

(4) Where, after all possible means of identification have been exhausted, the person specified in subsection 2 of this section cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner, the natural person who holds the position of a senior managing official is deemed as a beneficial owner.

(5) The obliged entity registers and keeps records of all actions taken in order to identify the beneficial owner under subsections 2 and 4 of this section.

(6) In the case of a trust, civil law partnership, community or legal arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such associations':
1) settlor or person who has handed over property to the asset pool;
2) trustee or manager or possessor of the property;
3) person ensuring and controlling the preservation of property, where such person has been appointed, or
4) the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.

(7) In the case of a person or an association of persons not specified in subsections 2 and 6 of this section, a member or members of the management board may be designated as a beneficial owner.

(8) 'Control via other means' means the exercising of dominant influence in accordance with the criteria set out in subsection 1 of § 27 of the Accounting Act.

(9) This section does not apply to:
1) a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information;
2) an apartment association provided for in the Apartment Ownership and Apartment Associations Act;
[RT I, 17.11.2017, 2 - entry into force 01.01.2018]
3) a building association provided for in the Building Association Act.

§ 10. Risk appetite

(1) 'Risk appetite' means the total of the exposure level and types of the obliged entity, which the obliged entity is prepared to assume for the purpose of its economic activities and attainment of its strategic goals, and which is established by the senior management of the obliged entity in writing.

(2) Upon application of subsection 1 of this section, account must be taken of the risks that the obliged entity is prepared to assume or that the obliged entity wishes to avoid in connection with the economic activities as well as qualitative and quantitative compensation mechanisms such as the planned revenue, measures applied with the help of capital or other liquid funds, or other factors such as reputation risks as well as legal and risks arising from money laundering and terrorist financing or other unethical activities.

(3) Upon application of subsection 1 of this section, the obliged entity determines at least the characteristics of the persons with whom the obliged entity wishes to avoid business relationships and with regard to which the obliged entity applies enhanced due diligence measures, and thereby the obliged entity assesses risks related to such persons and determines appropriate measures for mitigating these risks.

(4) Upon application of subsection 1 of this section, the management board of a credit institution or financial institution also determines whether business relationships will be established with persons from a country outside the European Economic Area or with e-residents.

Chapter 2
MANAGEMENT OF RISKS RELATING TO MONEY LAUNDERING AND TERRORIST FINANCING

Division 1

Assessment of Risks

§ 11. National risk assessment

(1) The national risk assessment:
1) provides for the needs of drafting and amending anti-money laundering and countering the financing of terrorism (hereinafter *AML/CFT*) legislation, other regulations of the field and related fields as well as guidelines of supervisory authorities;
2) specifies, among other things, the sectors, fields, transaction amounts and types and, where necessary, countries or jurisdictions with regard to which obliged entities must apply enhanced due diligence measures and, where necessary, clarifies the measures;
3) specifies, among other things, the sectors, fields, transaction amounts and types whereby the risk of money laundering and terrorist financing is smaller and where it is possible to apply simplified due diligence measures;
4) gives instructions to the ministries and authorities in their area of government regarding allocation of resources and setting of priorities for AML/CFT purposes.

(2) Upon implementation of subsection 1 of this section, relevant information, statistics and analyses which have been published or made available to the ministries or authorities in their area of government, including relevant risk assessments, reports and recommendations of international organisations and the European Commission are taken into account and collected, thereby taking account of data protection requirements.

(3) The generalised results of the national risk assessment are published on the website of the Ministry of Finance and immediately made available to obliged entities, the European Commission, European supervisory authorities and other Member States of the European Union.

(4) Based on the national risk assessment, the minister responsible for the field may by a regulation establish limit amounts, requirements for monitoring a business relationship or other risk-based restrictions aimed at mitigating the risks of money laundering or terrorist financing.

(5) In addition to the information specified in subsection 3 of this section, the Ministry of Finance publishes the aggregate statistics of the field of money laundering and terrorist financing on its website.

§ 12. AML/CFT Committee

(1) The AML/CFT Committee is a government committee whose function is to:
1) coordinate the preparation and updating of the national risk assessment;
2) prepare a plan of measures and activities mitigating the risks identified in the national risk assessment (hereinafter *action plan*), designating the authorities that apply the risk-mitigating measures and carry out the risk-mitigating activities as well as the time limits within which the measures must be applied and the activities must be carried out;
3) organise and check the implementation of the action plan;
4) based on clauses 1–3 of this subsection, develop AML/CFT policies and make legislative amendment proposals to the ministers responsible for the field and related fields;
5) pursue national cooperation in AML/CFT and in countering proliferation.

(2) The AML/CFT Committee consists of the minister responsible for the field, the secretary general and the secretaries general of the ministries responsible for the related fields, representatives of the Financial Intelligence Unit, Eesti Pank, Estonian Financial Supervision Authority, and representatives of other relevant bodies and governmental authorities.

(3) The AML/CFT Committee establishes a committee of the representatives of obliged entities (hereinafter *Market Participants Advisory Committee*) whose purpose is to advise the government committee in connection with the performance of its functions. In addition, ad hoc working groups and standing working groups of representatives of obliged entities and other experts may be established for performing the functions of the government committee. The rules of procedure and functions of the Market Participants Advisory Committee, ad hoc working groups and standing working groups are established and members are appointed by a directive of the minister responsible for the field.

(4) The number of the members and the rules of procedure of the AML/CFT Committee are established by a regulation of the Government of the Republic.

(5) The work of the AML/CFT Committee is organised by the Ministry of Finance.

§ 13. Management of risks arising from activities of obliged entity

(1) For the purpose of identification, assessment and analysis of risks of money laundering and terrorist financing related to their activities, obliged entities prepare a risk assessment, taking account of at least the following risk categories:
1) risks relating to customers;
2) risks relating to countries, geographic areas or jurisdictions;
3) risks relating to products, services or transactions;

4) risk relating to communication, mediation or products, services, transactions or delivery channels between the obliged entity and customers.

(2) The steps taken to identify, assess and analyse risks must be proportionate to the nature, size and level of complexity of the economic and professional activities of the obliged entity.

(3) As a result of the risk assessment, the obliged entity establishes:
1) fields of a lower and higher risk of money laundering and terrorist financing;
2) the risk appetite, including the volume and scope of products and services provided in the course of business activities;
3) the risk management model, including simplified and enhanced due diligence measures, in order to mitigate identified risks.

(4) The risk assessment specified in subsection 1 of this section and the establishment of the risk appetite specified in clause 2 of subsection 3 is documented, the documents are updated where necessary and based on the published results of the national risk assessment. At the request of the competent supervisory authority, the obliged entity submits the documents prepared on the basis of this section to the supervisory authority.

(5) The competent supervisory authority exercising supervision over the obliged person may, at the request of the obliged entity, except for an obliged entity subject to supervision by the Financial Supervision Authority, and in accordance with the national risk assessment decide that the preparation of a documented risk assessment is not mandatory where the specific risks characteristic of the obliged person are clear and understandable or where the risk assessment prepared by the competent supervisory authority or the national risk assessment has established the risks, risk appetite and risk management model of the field and the obliged entity implements these.

(6) The duties provided for in this section do not apply to notaries, auditors or to the obliged entities specified in subsections 3 and 4 of § 2 of this Act.

Division 2
Risk Management System of Obliged Entity

§ 14. Rules of procedure and internal control rules

(1) The obliged person establishes rules of procedure that allow for effective mitigation and management of, inter alia, risks relating to money laundering and terrorist financing, which are identified in the risk assessment prepared in accordance with § 13 of this Act. To follow the rules of procedure, the obliged entity establishes internal control rules that describe the internal control system including the procedure for the implementation of internal audit and, where necessary, compliance control, which sets out, inter alia, the procedure for employee screening. The rules of procedure must contain at least the following:
1) a procedure for the application of due diligence measures regarding a customer, including a procedure for the application of simplified due diligence measures specified in § 32 of this Act and of enhanced due diligence measures specified in § 36 of this Act;
2) a model for identification and management of risks relating to a customer and its activities and the determination of the customer’s risk profile;
3) the methodology and instructions where the obliged entity has a suspicion of money laundering and terrorist financing or an unusual transaction or circumstance is involved as well as instructions for performing the reporting obligation;
4) the procedure for data retention and making data available;
5) instructions for effectively identifying whether a person is a politically exposed person or a local politically exposed person subject to international sanctions or a person whose place of residence or seat is in a high-risk third country or country that meets the criteria specified in subsection 4 of § 37 of this Act;
6) the procedure for identification and management of risks relating to new and existing technologies, and services and products, including new or non-traditional sales channels and new or emerging technologies.

(2) The obliged entity arranges adherence to and implementation of the rules of procedure and internal control rules by the employees of the obliged entity.

(3) The rules of procedure and the internal control rules specified in subsection 1 of this section may be contained in a single document or in multiple documents, these must be proportionate to the nature, size and level of complexity of the economic and professional activities of the obliged entity and these must be established by the senior management of the obliged entity. The obliged entity must regularly check if the established rules of procedure and the internal control rules are up to date and, where necessary, establish new rules of procedure and internal control rules or make required modifications therein.

(4) Upon performance of the obligation provided for in clause 2 of subsection 1 of this section the credit institution and the financial institution takes account of the contents of the relevant instructions of the competent supervisory authority, European supervisory authorities and data protection supervisory authority.

(5) Where the obliged entity has the internal audit obligation, adherence to the rules of procedure and the internal control rules for the purposes of this Act must be checked in the course of an internal audit.

(6) The management board of a legal person that is an obliged entity, the director of a branch that is an obliged entity or, upon their absence, the obliged entity must ensure that the employees whose employment duties include the establishment of business relationships or the making of transactions are provided with training in the performance of the duties and obligations arising from this Act and such training must be provided when the employee commences performance of the specified employment duties, and thereafter regularly or when necessary. In training, information, inter alia, on the duties and obligations provided for in the rules of procedure, modern methods of money laundering and terrorist financing and the related risks, the personal data protection requirements, on how to recognise acts related to possible money laundering or terrorist financing, and instructions for acting in such situations must be given.

(7) The obliged entity, except for a credit institution or financial institution, may apply to the competent supervisory authority for partial or full release from the obligation to prepared documented rules of procedure and internal control rules. Upon making a decision, the competent supervisory authority takes account of the national risk assessment, the nature, scope and level of complexity of the obliged entity and whether the specific risks related to the obliged person are small or effectively managed in accordance with this Act, legislation adopted on the basis thereof and instructions of competent supervisory authorities.

(8) The minister responsible for the field may, by a regulation, establish more detailed requirements for the rules of procedure established by credit institutions and financial institutions, the internal control rules of controlling adherence thereto and implementation thereof.

(9) The duties and obligations provided for in this section do not apply to the obliged entities specified in subsections 3 and 4 of § 2 of this Act.

§ 15. Management of risks in group

(1) Upon application of § 14 of this Act it is expected that an obliged entity that is the parent undertaking of a group applies group-wide rules of procedure and the internal control rules for controlling adherence thereto regardless of whether all the undertakings of the group are located in one country or in different countries. This obligation includes, inter alia, the establishment of a group-wide procedure for exchanging information on AML/CFT and the establishment of similar rules for protection of personal data. The obliged entity ensures that group-wide rules of procedure and the internal control rules for controlling adherence thereto take to the appropriate extent account of the law of another Member State of the European Union which implements Directive (EU) 2015/849 of the European Parliament and of the Council, where the obliged entity has a representation, branch or majority-owned subsidiary in that Member State.

(2) Where the obliged entity has a representation, branch or majority-owned subsidiary in a third country where the minimum requirements for AML/CFT are not equivalent to those of Directive (EU) 2015/849 of the European Parliament and of the Council, the representation, branch and majority-owned subsidiary follow the rules of procedure and internal control rules complying with the requirements of this Act, including the requirements for protection of personal data, to the extent permitted by the law of the third country.

(3) Where the obliged entity identifies a situation where the law of the third country does not allow for implementing rules of procedure or internal control rules complying with the requirements of this Act in its representation, branch or majority-owned subsidiary, the obliged entity informs the competent supervisory authority thereof. The competent supervisory authority notifies the Member States and, where relevant, the European supervisory authorities where it has become evident in accordance with the first sentence of this subsection that the law of the third country does not allow for applying rules of procedure or internal control rules complying with the requirements of Directive (EU) 2015/849 of the European Parliament and of the Council.

(4) In the case specified in subsection 3 of this section, the obliged entity ensures the application of additional measures in the representation, branch or majority-owned subsidiary so that the risks relating to money laundering or terrorist financing are effectively managed in another manner, informing the competent supervisory authority of the measures taken. In such an event the competent supervisory authority has the right to issue a precept demanding, inter alia, that the obliged entity or its representation, branch or majority-owned subsidiary:
1) refrain from establishing new business relationships in the country;
2) terminate the existing business relationships in the country;
3) suspend the provision of the service in part or in full;
4) wind itself up;
5) apply other measures provided for in regulatory technical standards adopted by the European Commission on the basis of Article 45(7) of Directive (EU) 2015/849 of the European Parliament and of the Council.

(5) Within the group, information on a suspicion reported to the Financial Intelligence Unit may be shared, unless the Financial Intelligence Unit has ordered otherwise.

(6) An e-money institution or a payment service provider that operates in Estonia in a form other than a branch and the headquarters of which are in another Member State appoints, on the basis of an order made by the competent supervisory authority and in accordance with regulatory technical standards established on the basis of Article 45(9) of Directive (EU) 2015/849 of the European Commission, a central contact point in Estonia whose function is to ensure in the name of the e-money institution or payment service provider compliance with the requirements of this Act and, at the request of the competent supervisory authority, submits documents and information on its activities.

(7) Where a foreign service provider is an obliged entity and has a branch that has been registered in the Estonian commercial register or where a foreign service provider has a majority-owned subsidiary, it does not need to apply the group-wide rules of procedure or internal control rules to the extent that adherence thereto would be in conflict with the national risk assessment prepared on the basis of this Act or with requirements established in or on the basis of this Act.

§ 16. Cooperation and exchange of information

Obliged entities cooperate with one another and with state supervisory and law enforcement authorities in preventing money laundering and terrorist financing, thereby communicating information available to them and replying to queries within a reasonable time, following the duties, obligations and restrictions arising from legislation.

§ 17. Appointment of management board member in charge and compliance officer

(1) Where the obliged entity has more than one management board member, the obliged entity appoints a management board member who is in charge of implementation of this Act and legislation and guidelines adopted on the basis thereof.

(2) The management board of a credit institution and financial institution and the director of the branch of a foreign credit institution and financial institution registered in the Estonian commercial register appoint a person who acts as a contact person of the Financial Intelligence Unit (hereinafter *compliance officer*). A compliance officer of the credit institution or financial institution reports directly to the management board of the credit institution or financial institution and has the competence, means and access to relevant information across all the structural units of the credit institution or financial institution.

(3) The obliged entity who is not a credit institution or financial institution may appoint a compliance officer for performance of AML/CFT duties and obligations.

(4) An employee or a structural unit may perform the duties of a compliance officer. Where a structural unit performs the duties of a compliance officer, the head of the respective structural unit is responsible for performance of the given duties. The Financial Intelligence Unit and the competent supervisory authority are informed of the appointment of a compliance officer.

(5) Only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties of a compliance officer may be appointed as a compliance officer. The appointment of a compliance officer is coordinated with the Financial Intelligence Unit.

(6) The Financial Intelligence Unit has the right to receive information from a compliance officer or compliance office candidate, their employer and state databases for the purpose of verifying the suitability of the compliance officer or compliance officer candidate. Where, as a result of the check carried out by the Financial Intelligence Unit, it becomes evident that the person's reliability is under suspicion due to their past acts or omissions, the person's reputation cannot be considered impeccable and the obliged entity may extraordinarily terminate the compliance officer's employment contract due to the loss of confidence. Where the duties of a compliance officer are performed by a structural unit, the provisions of this subsection are applied to each employee of the structural unit.

(7) The duties of a compliance officer include, inter alia:
1) organisation of the collection and analysis of information referring to unusual transactions or transactions or circumstances suspected of money laundering or terrorist financing, which have become evident in the activities of the obliged entity;
2) reporting to the Financial Intelligence Unit in the event of suspicion of money laundering or terrorist financing;
3) periodic submission of written statements on compliance with the requirements arising from this Act to the management board of a credit institution or financial institution or to the director of the branch of a foreign credit institution or financial institution registered in the Estonian commercial register;
4) performance of other duties and obligations related to compliance with the requirements of this Act.

(8) A compliance officer has the right to:
1) make proposals to the management board of a credit or financial institution or to the director of the branch of a foreign credit or financial institution registered in the Estonian commercial register for amendment and modification of the rules of procedure containing AML/CFT requirements and organisation of training specified in subsection 6 of § 14 of this Act;
2) demand that a structural unit of the obliged entity eliminate within a reasonable time deficiencies identified in the implementation of the AML/CFT requirements;
3) receive data and information required for performance of the duties of a compliance officer;
4) make proposals for organisation of the process of submission of notifications of suspicious and unusual transactions;
5) receive training in the field.

(9) Where no compliance officer has been appointed, the duties of a compliance officer are performed by the management board of the legal person, a management board member appointed on the basis of subsection 1 of this section, the director of the branch of the foreign company registered in the Estonian commercial register or a self-employed person.

(10) The duties and obligations provided for in this section do not apply to the obliged entities specified in subsections 3 and 4 of § 2 of this Act.

§ 18. Relationships with shell banks

(1) 'Shell bank' means a credit institution or financial institution, or an institution that carries out activities equivalent to those carried out by credit institutions and financial institutions, incorporated in a jurisdiction in which it has no physical presence, involving meaningful mind and management, and which is unaffiliated with a regulated credit or financial group.

(2) Credit institutions and financial institutions are not allowed to establish or continue correspondent relationships with shell banks and such credit institutions or financial institutions that knowingly allow shell banks use their accounts.

(3) An agreement violating the prohibition specified in subsection 2 of this section is void.

Chapter 3
DUE DILIGENCE MEASURES

Division 1
Grounds for Application of Due Diligence Measures

§ 19. Obligation to apply due diligence measures

(1) The obliged entity applies due diligence measures:
1) upon establishment of a business relationship;
2) upon making or mediating occasional transactions outside a business relationship where a cash payment of over 15 000 euros or an equal amount in another currency is made, regardless of whether the financial obligation is performed in the transaction in a lump sum or in several related payments over a period of up to one year, unless otherwise provided by law;
3) upon verification of information gathered while applying due diligence measures or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered earlier while updating the relevant data;
4) upon suspicion of money laundering or terrorist financing, regardless of any derogations, exceptions or limits provided for in this Act.

(2) A trader applies due diligence measures at least every time a payment of over 10 000 euros or an equal sum in another currency is made to or by the trader in cash, regardless of whether the pecuniary obligation is performed in a lump sum or by way of several linked payments over a period of up to one year.

(3) A gambling operator applies due diligence measures at least upon payment of winnings, making of a bet or on both occasions where the sum given or receivable by the customer is at least 2000 euros or an equal sum in another currency, regardless of whether the pecuniary obligation is performed in a lump sum or by way of several linked payments over a period of up to one month.

(4) A payment service provider providing both the payer and the payee with a payment service identifies the customer in the case of each transfer of funds that meets the description provided for in Article 3(9) of Regulation (EU) No 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 (OJ L 141, 05.06.2015, pp 1–18) and whereby the sum of the pecuniary obligation exceeds 1000 euros, regardless of whether the pecuniary obligation is performed in a lump sum or by way of several linked payments over a period of up to one month.

(5) The obliged entity applies the due diligence measures provided in clauses 1–5 of subsection 1 of § 20 of this Act before each establishment of a business relationship or the making of each transaction outside a business relationship, unless otherwise provided for in this Act.

(6) Where the duty to apply due diligence measures depends on the exceeding of a certain sum, the due diligence measures must be applied as soon as the exceeding of the sum becomes known or, where the exceeding of the sum depends on the making of several linked payments, as soon as the sum is exceeded.

(7) The provisions of this Chapter regarding cash are also applicable to the performance of pecuniary obligations using a precious metal which is measured in bars or other units.

§ 20. Due diligence measures

(1) The obliged entity applies the following due diligence measures:
1) identification of a customer or a person participating in an occasional transaction and verification of the submitted information based on information obtained from a reliable and independent source, including using means of electronic identification and of trust services for electronic transactions;
2) identification and verification of a customer or a person participating in an occasional transaction and their right of representation;
3) identification of the beneficial owner and, for the purpose of verifying their identity, taking measures to the extent that allows the obliged entity to make certain that it knows who the beneficial owner is, and understands the ownership and control structure of the customer or of the person participating in an occasional transaction;
4) understanding of business relationships, an occasional transaction or act and, where relevant, gathering information thereon;
5) gathering information on whether a person is a politically exposed person, their family member or a person known to be close associate;
6) monitoring of a business relationship.

(2) Upon implementation of clause 4 of subsection 1 of this section, the obliged entity must understand the purpose of the business relationship or the purpose of the occasional transaction, identifying, inter alia, the permanent seat, place of business or place of residence, profession or field of activity, main contracting partners, payment habits and, in the case of a legal person, also the experience of the customer or person participating in the occasional transaction.

(3) In the case of an occasional transaction made outside of a business relationship, the obliged entity gathers information on the origin of the property used in the transaction, instead of applying clause 4 of subsection 1 of this section.

(4) Where relevant, the obliged entity also gathers information on the origin of the customer’s wealth.

(5) A person participating in a transaction made in economic or professional activities, a person participating in a professional act or a person using a professional service or a customer submits, at the request of the obliged entity, documents required for application of the due diligence measures specified in subsections 1–4 of this section and provides relevant information. A person participating in a transaction made in economic or professional activities, a person participating in a professional act or a person using a professional service or a customer certifies by signature, at the request of the obliged entity, the correctness of the submitted information and documents submitted for the application of the due diligence measures.

(6) The obliged entity applies all the due diligence measures specified in subsection 1 of this section with regard to a customer, but determines the scope and exact manner of their application and the need specified in subsections 3 and 4 of this section based on previously assessed risks of money laundering and terrorist financing or those relating to a specific business relationship or to an occasional transaction, act or person. Upon assessment of the application of the due diligence measures of the obliged entity, the principle of reasonableness provided for in the Law of Obligations Act is taken into account.

(7) Upon assessment of specific risks related to a customer specified in subsection 6 of this section, the obliged person determines, based on clause 2 of subsection 1 of § 14 of this Act, the risk profile of the customer or person participating in the transaction, taking account of the risk assessment drawn up on the basis of § 13 of this Act and at least the following factors:
1) information gathered by the obliged entity upon implementation of clause 4 of subsection 1 of this section;
2) the volume of the property deposited by the customer or the proprietary volume of the transaction or of transactions made in the course of a professional act;
3) the estimated duration of the business relationship.

(8) The obliged entity ensures that the due diligence measures applied by it, which are specified in its rules of procedure, comply with its risk assessment and that the obliged entity is prepared to explain them to the competent supervisory authority, including to the data protection supervisory authority.

§ 21. Identification of natural person, documents serving as basis thereof and data collected on customer

(1) The obliged entity identifies the customer and, where relevant, their representative and retains the following data on the person and, where relevant, their representative:
1) name;
2) personal identification code or, if none, the date and place of birth and the place of residence or seat;
3) information on the identification and verification of the right of representation and scope thereof and, where the right of representation does not arise from law, the name of the document serving as the basis for the right of representation, the date of issue, and the name of the issuer.

(2) The obliged entity verifies the correctness of the data specified in clauses 1 and 2 of subsection 1 of this section, using information originating from a credible and independent source for that purpose. Where the identified person has a valid document specified in subsection 3 of this section or an equivalent document, the person is identified and the person's identity is verified on the basis of the document or using means of electronic identification and trust services for electronic transactions, and the validity of the document appears from the document or can be identified using means of electronic identification and trust services for electronic transactions, no additional details on the document need to be retained.

(3) The obliged entity identifies a natural person based on the following documents:
1) a document specified in subsection 2 of § 2 of the Identity Documents Act;
2) a valid travel document issued in a foreign country;
3) a driving licence that meets the requirements provided for in subsection 1 of § 4 of the Identity Documents Act, or
4) a birth certificate specified in § 30 of the Vital Statistics Registration Act in the case of a person below the age of seven years.

(4) Where the original document specified in subsection 3 of this section is not available, the identity can be verified on the basis of a document specified in subsection 3, which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.

§ 22. Identification of legal person, documents serving as basis thereof and data collected on customer

(1) The obliged person identifies a legal person registered in Estonia, the branch of a foreign company registered in Estonia and a foreign legal person and retains the following details on the legal person:
1) the name or business name of the legal person;
2) the registry code or registration number and the date of registration;
3) the names of the director, members of the management board or other body replacing the management board, and their authorisation in representing the legal person;
4) the details of the telecommunications of the legal person.

(2) The obliged entity verifies the correctness of the data specified in clauses 1 and 2 of subsection 1 of this section, using information originating from a credible and independent source for that purpose. Where the obliged entity has access to the commercial register, register of non-profit associations and foundations or the data of the relevant registers of a foreign country, the submission of the documents specified in subsection 3 of this section does not need to be demanded from the customer.

(3) The obliged entity identifies a legal person based on the following documents:
1) the registry card of the relevant register;
2) the registration certificate of the relevant register, or
3) a document equal to the document specified in clause 1 or 3 of this section.

(4) Where the original document specified in subsection 3 of this section is not available, the identity can be verified on the basis of a document specified in subsection 3, which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification and trust services for electronic transactions, thereby using at least two different sources for verification of data in such an event.

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

§ 23. Monitoring of business relationship

(1) The obliged entity establishes principles for monitoring a business relationship established in economic or professional activities (hereinafter *monitoring of business relationship*) upon application of § 14 of this Act.

(2) The monitoring of a business relationship must include at least the following:
1) checking of transactions made in a business relationship in order ensure that the transactions are in concert with the obliged entity's knowledge of the customer, its activities and risk profile;

2) regular updating of relevant documents, data or information gathered in the course of application of due diligence measures;
3) identifying the source and origin of the funds used in a transaction;
4) in economic or professional activities, paying more attention to transactions made in the business relationship, the activities of the customer and circumstances that refer to a criminal activity, money laundering or terrorist financing or that a likely to be linked with money laundering or terrorist financing, including to complex, high-value and unusual transactions and transaction patterns that do not have a reasonable or visible economic or lawful purpose or that are not characteristic of the given business specifics;
5) in economic or professional activities, paying more attention to the business relationship or transaction whereby the customer is from a high-risk third country or a country or territory specified in subsection 4 of § 37 of this Act or whereby the customer is a citizen of such country or whereby the customer's place of residence or seat or the seat of the payment service provider of the payee is in such country or territory.

(3) Upon performance of the duty provided for in clause 4 of subsection 2 of this section, inter alia, the nature, reason and background of the transactions as well as other information that allows for understanding the substance of the transactions must be identified and more attention must be paid to these transactions.

Division 2
Variations of Application of Due Diligence Measures

§ 24. Reliance on data gathered by other person and outsourcing of application of due diligence measures

(1) The obliged entity may, in the event of the partial or full performance of one or several of the duties provided for in clauses 1–4 of subsection 1 of § 20 of this Act, rely on data and documents gathered by another person, where all the following criteria are met:
1) the obliged entity gathers from the other person at least information on who is the person establishing the business relationship or making the transaction, their representative and the beneficial owner, as well as what is the purpose and nature of the business relationship or transaction;
2) the obliged entity has ensured that, where necessary, it is able to immediately obtain all the data and documents whereby it relied on data gathered by another person;
3) the obliged entity has established that the other person who is relied on is required to comply and actually complies with requirements equal to those established by Directive (EU) 2015/849 of the European Parliament and of the Council, including requirements for the application of due diligence measures, identification of politically exposed persons and data retention, and is under or is prepared to be under state supervision regarding compliance with the requirements;
4) the obliged entity takes sufficient measures to ensure compliance with the criteria provided for in clause 3 of this subsection.

(2) In addition to the provisions of subsection 1 of this section, the obliged entity may also outsource an activity related to the implementation of clauses 1–4 of subsection 1 of § 20 of this Act to:
1) another obliged entity;
2) an organisation, association or union whose members are obliged entities, or
3) another person who applies the due diligence measures and data retention requirements provided for in this Act and who is subject to or is prepared to be subject to AML supervision or financial supervision in a contracting state of the European Economic Area regarding compliance with requirements.

(3) To outsource an activity, the obliged entity concludes a written contract with a person specified in subsection 2 of this section. The contract ensures that:
1) the outsourcing of the activity does not impede the activities of the obliged entity or performance of the duties and obligations provided in this Act;
2) the third party performs all the duties of the obliged entity relating to the outsourcing of the activity;
3) the outsourcing of the activity does not impede exercising supervision over the obliged entity;
4) the competent authority can exercise supervision over the person carrying out the outsourced activity via the obliged entity, including by way of an on-site inspection or another supervisory measure;
5) the person specified in subsection 2 of this section has the required knowledge and skills and the ability to comply with the requirements provided for in this Act;
6) the obliged entity has the right to, without limitations, inspect compliance with the requirements provided for in this Act;
7) documents and data gathered for compliance with the requirements arising from this Act are retained and, at the request of the obliged entity, copies of documents relating to the identification of a customer and its beneficial owner or copies of other relevant documents are handed over or submitted to the competent authority immediately.

(4) Information on the conclusion and termination of an outsourcing contract is made available to the competent supervisory authority in advance. Upon submission of information, the obliged entity indicates, among other

things, the scope of the outsourced activity. At the request of the competent supervisory authority, the obliged entity submits the contract of outsourcing of the activity.

(5) In a situation where the obliged entity relies on or outsources an activity to a person belonging to the same group, which has been established in a country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council apply, including requirements for the application of due diligence measures, identification of politically exposed persons and data retention, and where group-based supervision is exercised over the group, the requirements provided for in clause 3 of subsection 1 and in clause 5 of subsection 3 of this section do not need to be applied.

(6) The obliged entity is not allowed to rely on or outsource activities to a person who has been established in a high-risk third country.

(7) The obliged person who relies on data gathered by another person or who has outsourced an activity to another person is responsible for compliance with requirements arising from this Act.

§ 25. Variations of due diligence measures applied by credit institution, financial institution and Eesti Pank

(1) A credit institution and a financial institution is not allowed to provide services that can be used without identifying the person participating in the transaction and without verifying the submitted information, except in the events specified in § 27 of this Act. Credit institutions and financial institutions are required to open an account and keep an account only in the name of the account holder.

(2) Credit institutions and financial institutions are not allowed to conclude a contract or make a decision to open an anonymous account or a savings book. A transaction in violation of the prohibition is void.

(3) Eesti Pank applies the due diligence measures specified in clauses 1–4 of subsection 1 of § 20 of this Act.

(4) Eesti Pank applies the due diligence measures specified in clauses 1–4 of subsection 1 of § 20 of this Ac always when there is doubt as to the sufficiency or truthfulness of documents or data previously gathered in the course of identification of a person, verification of submitted information or updating the relevant details as well as in the event of suspicion of terrorist financing.

§ 26. Due diligence measures applicable to life insurance

(1) In the case of life insurance, a credit institution and a financial institution applies the due diligence measures specified in § 20 of this Act with the following variations:
1) the name of the beneficiary determined in the insurance contract is identified immediately after the determination of the person or after learning of the person;
2) where the beneficiary is not determined by name, but based on certain characteristics or in another manner, sufficient data must be gathered on the circle of persons determined in such a manner so that it is proven that the identity of the beneficiary can be established at the time of making a payment.

(2) In the case of subsection 1 of this section, the identity of the beneficiary is verified at the time of making a payment.

(3) Where, by agreement with the obliged entity, a policyholder assigns their rights and obligations under a life insurance contract to a third party, the obliged entity must identify the assignee of the contract at the moment of assignment of the contract.

§ 27. Due diligence measures applicable to limited-use accounts

(1) By way of exception, a credit institution, financial institution or central securities depositor can open an account, including a securities account, before the application of the due diligence measures specified in clauses 1–3 of subsection 1 of § 20 of this Act where transactions cannot be made by the customer or in the name of the customer with the property held on the account until the full application of the due diligence measures specified in clauses 1–3 of subsection 1 of § 20 of this Act, thereby applying the due diligence measures as soon as reasonably possible.

(2) In accordance with the procedure established on the basis of clause 1 of subsection 4 of § 67 of the Commercial Code, a credit institution can, on the basis of personal data automatically verified by the registrar via the computer network or via a notary authorised on the basis of subsection 4 of § 520 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 1–4 of subsection 1 of § 20 of this Act have been taken. Representatives of the company must allow the credit institution to apply the due diligence measures and conclude a settlement agreement within six months following the opening of the account.

§ 28. Due diligence measures applicable to trust fund and legal arrangement

In addition to the due diligence measures specified in subsection 1 of § 21 of this Act, a credit institution or financial institution gathers enough information on the beneficiaries of a trust fund or a legal arrangement, which have been determined based on certain characteristics or type, in order to be certain that it is able to identify the beneficiary at the time of making a payment or once the beneficiary exercises their rights.

§ 29. Due diligence measures applied by non-profit association and foundation

(1) The persons specified in subsection 3 of § 2 of this Act apply the due diligence measures specified in clauses 1–4 of subsection 1 of § 20 of this Act.

(2) The persons specified in subsection 3 of § 2 of this Act apply the due diligence measures specified in clauses 1–4 of subsection 1 of § 20 of this Ac always when there is doubt as to the sufficiency or truthfulness of documents or data previously gathered in the course of identification of a person, verification of submitted information or updating the relevant details as well as in the event of suspicion of money laundering or terrorist financing.

§ 30. Variations of due diligence measures applied by legal service provider

(1) Where a notary identifies a person and applies other due diligence measures, the Notarisation Act and the Notaries Act are followed, taking account of the variations provided for in this Act.

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

(3) In the case specified in subsection 2 of this section, the application of due diligence measures must be completed as soon as possible after the first contact and before taking binding measures.

§ 31. Identification of person and verification of data using information technology means

(1) A credit institution and a financial institution must identify a person and verify data with the help of information technology means where a business relationship is established with an e-resident or a person from a country outside the European Economic Area or whose place of residence or seat is in such country and where the due diligence measures are not applied while being physically in the same place as the person or their representative.

(2) A credit institution and a financial institution must identify a person and verify data with the help of information technology means where a business relationship is established with a person from a contracting state of the European Economic Area or whose place of residence or seat is in such a country and whose total sum of outgoing payments relating to a transaction or a service contract exceeds 15 000 euros per calendar month or, in the case of a customer who is a legal person, 25 000 euros per calendar month, and where the due diligence measures are not applied while being physically in the same place as the person or their representative.

(3) A document issued by the Republic of Estonia for digital identification of a person or another electronic identification system with assurance level ‘high’ which has been added to the list published in the Official Journal of the European Union based on Article 9 of Regulation (EC) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.08.2014, pp 73–114) is used for identification of a person and verification of data with the help of information technology means.

(4) Where a person is a foreign national, the identity document issued by the competent authority of the foreign country must be used for the identification of the person and verification of data in addition to the means specified in subsection 3 of this section.

(5) Additionally, information originating from a credible and independent source is used for identifying a person and verifying data. To identify an e-resident and verify data, a credit institution and a financial institution has the right to use personal identification data entered in the database of identity documents.

(6) The technical requirements of and procedure for identification of persons and verification of data using information technology means are established by a regulation of the minister responsible for the field.

(7) The regulation specified in subsection 6 of this section sets out in greater detail at least requirements for disclosure of information, rules of procedure applicable to the establishment of a business relationship and to the making of an occasional 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 photograph 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, and, based on the national risk assessment specified in § 11 of this Act, the regulation may establish limits different from the ones specified in subsection 2 of this section to situations where the provisions of this section do not need to be applied.

Division 3
Simplified Due Diligence Measures

§ 32. Application of simplified due diligence measures

(1) The obliged entity may apply simplified due diligence measures where a risk assessment prepared on the basis of subsection 7 of § 20 and §§ 11, 13 and 34 of this Act identifies that, in the case of the economic or professional activity, field or circumstances, the risk of money laundering or terrorist financing is lower than usual.

(2) Before the application of simplified due diligence measures to a customer, the obliged entity establishes that the business relationship, transaction or act is of a lower risk and the credit institution and financial institution attribute to the transaction, act or customer a lower degree of risk.

(3) The application of simplified due diligence measures is permitted to the extent that the obliged entity ensures sufficient monitoring of transactions, acts and business relationships, so that it would be possible to identify unusual transactions and allow for notifying of suspicious transactions in accordance with the procedure established in § 49 of this Act.

§ 33. Conditions of application of simplified due diligence measures

(1) Upon simplified implementation of clauses 1 and 2 of subsection 1 of § 20 of this Act, the identity of a customer or of the customer's representative may be verified on the basis of information obtained from a credible and independent source also at the time of establishment of the business relationship, provided that it is necessary for not disturbing the ordinary course of business. In such an event the verification of identity must be carried out as quickly as possible and before the taking of binding measures.

(2) Upon implementation of clauses 3–5 of subsection 1 of § 20 of this Act, the obliged entity may choose the extent of performance of the duty and the need to verify the information and data used therefore with the help of a credible and independent source.

(3) Clause 6 of subsection 1 of § 20 of this Act may be applied in accordance with the simplified procedure, provided that a factor characterising a lower risk has been established and ay least the following criteria are met:
1) a long-term contract has been concluded with the customer in writing, electronically or in a form reproducible in writing;
2) payments accrue to the obliged entity in the framework of the business relationship only via an account held in a credit institution or the branch of a foreign credit institution registered in the Estonian commercial register or in a credit institution established or having its place of business in a contracting state of the European Economic Area or in a country that applies requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council;
3) the total value of incoming and outgoing payments in transactions made in the framework of the business relationship does not exceed 15 000 euros a year.

§ 34. Factors characterising lower risk

(1) Before the application of simplified due diligence measures, factors referring to a lower risks are taken into account and the obliged entity determines whether these factors will be implemented on the whole, in part or as separate grounds.

(2) Upon assessment of factors referring to a lower risk in accordance with subsection 1 of this section, the following is deemed a situation reducing risks relating to the customer type:
1) the customer is a company listed on a regulated market, which is subject to disclosure obligations that establish requirements for ensuring sufficient transparency regarding the beneficial owner;
2) the customer is a legal person governed by public law established in Estonia;
3) the customer is a governmental authority or another authority performing public functions in Estonia or a contracting state of the European Economic Area;
4) the customer is an institution of the European Union;
5) the customer is a credit institution or financial institution acting on its own behalf or a credit institution or financial institution located in a contracting state of the European Economic Area or a third country, which in its country of location is subject to requirements equal to those established in Directive (EU) 2015/849 of the European Parliament and of the Council and subject to state supervision;
6) a person who is a resident of a country or geographic area having the characteristics specified in clauses 1–4 of subsection 3 of this section.

(3) Upon assessment of factors referring to a lower risk in accordance with subsection 1 of this section, at least the following situations where the customer is from or the customer's place of residence or seat is in, may be deemed a factor reducing geographic risks:
1) a contracting state of the European Economic Area;
2) a third country that has effective AML/CFT systems;
3) a third country where, according to credible sources, the level of corruption and other criminal activity is low;
4) a third country where, according to credible sources such as mutual evaluations, reports or published follow-up reports, AML/CFT requirements that are in accordance with the updated recommendations of the Financial Action Task Force (FATF), and where the requirements are effectively implemented.

§ 35. Variations of application of simplified due diligence measures by credit institution and financial institution

(1) Upon identifying factors characterising a smaller risk and choosing simplified due diligence measures, credit institutions and financial institutions take into account the guidelines of the European supervisory authorities regarding risk factors.

(2) Under subsection 1 of § 34 of this Act, at least the following factors may be deemed factors reducing risks relating to the product, service, transaction or delivery channels upon assessment of factors referring to a lower risk:
1) a life insurance contract with a small insurance premium;
2) an insurance policy for a pension scheme where there is no early surrender option and the policy cannot be used as collateral;
3) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
4) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
5) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits, in addition to clause 3 of subsection 3 of § 33 of this Act, or transparency of ownership;
6) basic payment services relating to a liability account.

Division 4
Enhanced Due Diligence Measures

§ 36. Application of enhanced due diligence measures

(1) The obliged entity applies enhanced due diligence measures in order to adequately manage and mitigate a higher-than-usual risk of money laundering and terrorist financing.

(2) Enhanced due diligence measures are applied always when:
1) upon identification of a person or verification of submitted information, there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
2) the person participating in the transaction or professional act made in economic or professional activities, the person using the professional service or the customer is a politically exposed person, except for a local politically exposed person, their family member or a close associate;
3) the person participating in the transaction or professional act made in economic or professional activities, the person using the professional service or the customer is from a high-risk third country or their place of residence or seat or the seat of the payment service provider of the payee is in a high-risk third country;
4) the customer or the person participating in the transaction or the person using the professional service is from such country or territory or their place of residence or seat or the seat of the payment service provider of the payee is in a country or territory that, according to credible sources such as mutual evaluations, reports or published follow-up reports, has not established effective AML/CFT systems that are in accordance with the recommendations of the Financial Action Task Force, or that is considered a low tax rate territory.

(3) The obliged entity applies enhanced due diligence measures also where a risk assessment prepared on the basis of subsection 6 of § 20 and §§ 11, 13 and 37 of this Act identifies that, in the case of the economic or professional activity, field or factors, the risk of money laundering or terrorist financing is higher than usual.

(4) Enhanced due diligence measures do not need to be applied regarding the branch of an obliged entity established in a contracting state of the European Economic Area or a majority-owned subsidiary seated in a high-risk third country, provided that the branch and the majority-owned subsidiary fully comply with the group-wide procedures in accordance with § 15 of this Act and the obliged entity assesses that the waiver to apply enhanced due diligence measures does not entail major additional risks of money laundering and terrorist financing.

§ 37. Factors characterising higher risk

(1) In addition to the events specified in subsection 2 of § 36 of this Act, at least the factors referring to a higher risk of money laundering and terrorist financing specified in subsections 2–4 of this section are taken into account upon application of enhanced due diligence measures. The obliged entity determines in rules of procedure whether it will apply the factors on the whole, in part or as separate grounds for the purpose of application of enhanced due diligence measures.

(2) Upon assessment of factors referring to a higher risk in accordance with subsection 1 of this section, the following is deemed a situation increasing risks related to the customer as a person:
1) the business relationship foundations based on unusual factors, including in the event of complex and unusually large transactions and unusual transaction patterns that do not have a reasonable, clear economic or lawful purpose or that are not characteristic of the given business specifics;
2) the customer is a resident of a higher-risk geographic area listed in subsection 4 of this section;
3) the customer is a legal person or a legal arrangement, which is engaged in holding personal assets;
4) the customer is a cash-intensive business;
5) the customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;
6) the ownership structure of the customer company appears unusual or excessively complex, given the nature of the company's business.

(3) Upon assessment of factors referring to a higher risk in accordance with subsection 1 of this section, in particular the following is deemed a situation increasing risks related to the product, service, transaction or delivery channel:
1) private banking;
2) provision of a product or making or mediating of a transaction that might favour anonymity;
3) payments received from unknown or unassociated third parties;
4) a business relationship or transaction that is established or initiated in a manner whereby the customer, the customer's representative or party to the transaction is not met physically in the same place and whereby § 31 of this Act is not applied as a safeguard measure;
5) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

(4) Upon assessment of factors referring to a higher risk in accordance with subsection 1 of this section, in particular as situation where the customer, a person involved in the transaction or the transaction itself is connected with a following country or jurisdiction is deemed a factor increasing the geographical risk:
1) that, according to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective AML/CFT systems;
2) that, according to credible sources, has significant levels of corruption or other criminal activity;
3) that is subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
4) that provides funding or support for terrorist activities, or that has designated terrorist organisations operating within their country, as identified by the European Union or the United Nations.

(5) Upon selection of enhanced due diligence measures, a credit institution and a financial institution takes into account, in addition to subsections 2–4 of this section, relevant guidelines of the European supervisory authorities regarding risk factors.

§ 38. Additional due diligence measures

(1) The obliged entity chooses additional due diligence measures in order to manage and mitigate an established risk of money laundering and terrorist financing that is higher than usual.

(2) To perform the duties provided for in subsection 1 of this section, the obliged entity may, among other things, apply one or several of the following due diligence measures:
1) verification of information additionally submitted upon identification of the person based on additional documents, data or information originating from a credible and independent source;
2) gathering additional information on the purpose and nature of the business relationship, transaction or operation and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;
3) gathering additional information and documents regarding the actual execution of transactions made in the business relationship in order to rule out the ostensibility of the transactions;
4) gathering additional information and documents for the purpose of identifying the source and origin of the funds used in a transaction made in the business relationship in order to rule out the ostensibility of the transactions;
5) the making of the first payment related to a transaction via an account that has been opened in the name of the person or customer participating in the transaction in a credit institution registered or having its place of business in a contracting state of the European Economic Area or in a country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council are in force;
6) the application of due diligence measures regarding the person or their representative while being at the same place as the person or their representative.

(3) Upon application of enhanced due diligence measures, the obliged entity must apply the monitoring of a business relationship more frequently than usually, including reassess the customer's risk profile not later than six months after the establishment of the business relationship.

(4) In addition to the provisions of this section, credit institutions and financial institutions take into account the guidelines of the European supervisory authorities upon selection of due diligence measures.

§ 39. Enhanced due diligence measures applied to transaction made with natural and legal persons operating in high-risk third country

(1) Where the obliged entity comes in contact with a high-risk third country via a person participating in a transaction made in the obliged entity's economic or professional activities, via a person participating in a professional act, via a person using a professional service or via a customer, the obliged entity applies the following due diligence measures:
1) gathering additional information about the customer and its beneficial owner;
2) gathering additional information on the planned substance of the business relationship;
3) gathering information on the origin of the funds and wealth of the customer and its beneficial owner;
4) gathering information on the underlying reasons of planned or executed transactions;
5) receiving permission from the senior management to establish or continue a business relationship;
6) improving the monitoring of a business relationship by increasing the number and frequency of the applied control measures and by choosing transaction indicators that are additionally verified.

(2) In addition to subsection 1 of this section, the obliged entity may demand that a customer make a payment from an account held in the customer's name in a credit institution of a contracting state of the European Economic Area or in a third country that implements requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council.

(3) In addition to subsection 1 of this section, a credit institution or a financial institution applies one or several of the following due diligence measures:
1) winding up its branch or representation in a high-risk third country;
2) carrying out a special audit in a subsidiary or branch of the credit institution or financial institution in a high-risk third country;
3) assessing and, where necessary, terminating a correspondent relationship with an obliged entity of a high-risk third country.

§ 40. Correspondent relationship with credit institution of third country

(1) In the case of a cross-border correspondent relationship with a respondent institution of a third country, a credit institution or a financial institution takes, in addition to the due diligence measures provided for in subsection 1 of § 20 of this Act, the following due diligence measures:
1) gathering sufficient information on the respondent institution in order to fully understand the nature of the activities of the respondent institution and, based on publicly available information, make a decision on the reputation and supervision quality of the relevant institution, including by researching whether any proceedings have been initiated against the institution in connection with violation of AML/CFT legislation;
2) assessment of AML/CFT control systems implemented in the respondent institution;
3) receiving prior approval from the senior management to establish a new correspondent relationship;
4) documentation of the relevant duties and obligations of both institutions;
5) in the case of payable-through accounts, making certain that the respondent institution has verified the identity of the customers who have direct access to the accounts of the correspondent institution, applies due diligence measures to them at all times and, upon request is able to present the relevant due diligence measures applied to the customer.

(2) A credit institution or a financial institution as an obliged entity who renders a service to another credit institution or financial institution in a correspondent relationship provided for in § 7 of this Act where the customers of the credit institution or financial institution receiving the service benefit from the service (hereinafter *beneficial customer*) does not need to apply the due diligence measures provided for in § 20 of this Act with regard to the beneficial customers where the obliged entity:
1) has established that the credit institution or financial institution who is a customer is itself required to apply and actually applies measures equal to the requirements provided for in this Act, including requirements for the application of due diligence measures, identification of politically exposed persons and data retention, and is under financial supervision;
2) is aware of the risk structure of the beneficial customers and makes certain that the related risk is in accordance with the risk appetite of the obliged entity;
3) has ensured by a contract that, where necessary, it is able to immediately obtain all data and documents in order to identify the person who ultimately benefits from the transaction;
4) takes sufficient measures to ensure compliance with the criteria provided for in clause 1 of this subsection.

(3) The obliged entity is prohibited to apply subsection 2 of this section where the credit institution or financial institution who is a customer has been established in a high-risk third country.

(4) The obliged entity applying subsection 2 of this section is responsible for compliance with the requirements arising from this Act.

§ 41. Transactions with politically exposed person

(1) In a situation where a person participating in a transaction made in economic or professional activities, a person participating in a professional act, a person using a professional service, a customer or their beneficial owner is a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person, the obliged entity applies the following due diligence measures in addition to the due diligence measures provided for in subsection 1 of § 20 of this Act:
1) obtains approval from the senior management to establish or continue a business relationship with the person;
2) applies measures to establish the origin of the wealth of the person and the sources of the funds that are used in the business relationship or upon making occasional transactions;
3) monitors the business relationship in an enhanced manner.

(2) In addition to the application of the due diligence measures specified in § 26 of this Act, the obliged entity establishes not later than upon making a payment whether the beneficiary of the life insurance policy or the beneficial owner of the beneficiary is a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person. Upon assignment of a life insurance contract in accordance with subsection 3 of § 26 of this Act, the obliged entity identifies the aforementioned facts regarding the assignee of the contract and their beneficial owner at the moment of assignment of the contract. Where the obliged entity identifies a politically exposed person, a family member of a politically exposed person or a person known to be a close associated of a politically exposed person, the obliged entity applies the following due diligence measures in addition to the due diligence measures provided for in subsection 1 of § 20 of this Act:
1) informing the senior management before making payments under the insurance policy;
2) checking the entire business relationship in detail.

(3) Where a politically exposed person no longer performs important public functions placed upon them, the obliged entity must at least within 12 months take into account the risks that remain related to the person and apply relevant and risk sensitivity-based measures as long as it is certain that the risks characteristic of politically exposed persons no longer exist in the case of the person.

(4) The obliged entity does not need to apply the due diligence measures provided for in this section with regard to a local politically exposed person, their family member or a person known to be their close associate where there are no other factors that refer to a higher-than-usual risk.

Division 5
Consequences of Failure to Apply Due Diligence Measures

§ 42. Consequences of impossibility to identify person, their representative or beneficial owner

(1) The obliged entity is prohibited to establish a business relationship or allow for making or closing an occasional transaction where the obliged entity is unable to comply with the due diligence measures provided for in clause 1, 2 or 3 of subsection 1 of § 20 of this Act or where the obliged entity suspects money laundering or terrorist financing.

(2) The obliged entity is prohibited to establish a business relationship or make a transaction with a person whose capital consists of bearer shares or other bearer securities.

(3) A payment service provider is prohibited to follow the customer’s payment instruction or make funds available where the payment service provider is unable to comply with the duty provided for in subsection 4 of § 19 of this Act.

(4) Where the obliged entity has a business relationship with a customer in a situation provided for in subsections 1–3 of this section, the refusal by the customer to provide information or documents required for the application of due diligence measures is deemed a fundamental breach of the contract and the obliged entity has the obligation to extraordinarily terminate the long-term contract serving as the basis for the business relationship and to notify the Financial Intelligence Unit of the suspicious transaction relating to the customer in accordance with § 49 of this Act. The business relationship is deemed terminated as of the submission of a termination notice to the customer after which the obliged entity makes the services completely unavailable to the customer.

(5) An agreement violating the prohibition specified in subsections 1–3 of this section is void.

(6) The provisions of subsections 1–5 are not applied where the obliged entity has notified the Financial Intelligence Unit of the establishment of a business relationship, transaction or an attempted transaction in accordance with the procedure provided for in § 49 of this Act and received from the Financial Intelligence Unit a specific instruction to continue the business relationship, the establishment of the business relationship or the transaction.

§ 43. Consequences of Failure to Apply Other Due Diligence Measures

(1) The obliged entity has the right to refuse to make a transaction where a person participating in a transaction, a person participating in a professional act, a person using a professional service or a customer, in spite of a respective request, does not submit documents and relevant information or data or documents proving the origin of the property constituting the object of the transaction or where, based on the submitted data and documents, the obliged entity comes to suspect money laundering or terrorist financing or the commission of related offences or an attempt at such activity.

(2) The obliged entity has the right to extraordinarily and without advance notification terminate the long-term contract serving as the basis for a business relationship:
1) upon refusal to issue an e-resident's digital identity card or where its validity is suspended or where it is declared invalid on the ground provided for in subsection 2 or 3 of § 20[6] of the Identity Documents Act;
2) in the events specified in subsection 1 of this section.

(3) Where, on the conditions described in subsection 1 or 2 of this section, the omission of a transaction would be impossible or where the omission of a transaction or termination of a business relationship might impede efforts made to catch persons benefiting from a suspicious transaction, the obliged entity may still make the transaction or continue the business relationship, informing the Financial Intelligence Unit thereof immediately after making the transaction or deciding to continue the business relationship in accordance with the procedure provided for in § 49 of this Act.

§ 44. Restrictions on transfer of customer's property

(1) Upon implementation of the provisions of this Division, the obliged entity may transfer the customer's property only to an account opened in a credit institution or the 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 country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council are in force. By way of exception, the property may be transferred to an account other than the customer's account, notifying the Financial Intelligence Unit thereof at least seven working days in advance and provided that the Financial Intelligence Unit does not give a different order.

(2) Upon opening an account to a company established in the manner provided for in subsection 2 of § 27 of this Act, subsection 1 of this section is applied, unless the Financial Intelligence Unit has established a different procedure by a precept made on the basis of § 55 of this Act. Subsection 6 of § 720 of the Law of Obligations Act does not apply to the implementation of this subsection.

§ 45. Variations upon provision of legal service

The provisions of this Division do not apply to a notary, enforcement officer, bankruptcy trustee, auditor, attorney or other legal service provider, provider of accounting services or provider of advisory services in the field of accounting or taxation where the person is involved in assessing the customer's legal status or in performing duties as the customer's defence counsel or representative in court proceedings or in connection therewith, including in connection with giving advance on the initiation or avoidance of proceedings.

Chapter 4
GATHERING, RETAINING AND PROTECTING DATA

§ 46. Registration of data

(1) The obliged entity registers the transaction date or period and a description of the substance of the transaction.

(2) In addition to the data specified in subsection 1, the obliged entity registers:
1) information on the circumstance of the obliged entity's refusal to establish a business relationship or make an occasional transaction;
2) the circumstances of a waiver to establish a business relationship or make a transaction, including. an occasional transaction, on the initiative of a person participating in the transaction or professional act, a person

using the official service or a customer where the waiver is related to the application of due diligence measures by the obliged entity;
3) information according to which it is not possible to take the due diligence measures provided for in subsection 1 of § 20 of this Act using information technology means;
4) information on the circumstances of termination of a business relationship in connection with the impossibility of application of the due diligence measures;
5) information serving as the basis for the duty to report under § 49 of this Act;
6) upon making transactions with a civil law partnership, community or another legal arrangement, trust fund or trustee, the fact that the person has such status, an extract of the registry card or a certificate of the registrar of the register where the legal arrangement has been registered.

(3) In addition to the information provided for in subsection 1 of this section, a credit institution, financial institution and central securities depository register 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 acceptance of property for depositing, the deposition number and the market price of the property on the date of deposition or a detailed description of the property where the market price 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 conclusion of a life insurance policy, the account number debited to the extent of the first insurance premium;
6) upon making a disbursement under a life insurance policy, the account number that was credited to the extent of the disbursement amount;
7) in the case of payment intermediation, the details the communication of which is mandatory under Regulation (EU) No 2015/847 of the European Parliament and of the Council;
8) in the case of another transaction, the transaction amount, the currency and the account number.

§ 47. Preservation of data

(1) The obliged entity must retain the originals or copies of the documents specified in §§ 21, 22 and 46 of this Act, which serve as the basis for identification and verification of persons, and the documents serving as the basis for the establishment of a business relationship no less than five years after termination of the business relationship.

(2) During the period specified in subsection 1 of this section, the obliged entity must also retain the entire correspondence relating to the performance of the duties and obligations arising from this Act and all the data and documents gathered in the course of monitoring the business relationship as well as data on suspicious or unusual transactions or circumstances which the Financial Intelligence Unit was not notified of.

(3) The obliged entity must retain the documents prepared with regard to a transaction on any data medium and the documents and data serving as the basis for the notification obligations specified in § 49 of this Act for no less than five years after making the transaction or performing the duty to report.

(4) The obliged entity must retain the documents and data specified in subsections 1–3 of this section in a manner that allows for exhaustively and immediately replying to the enquiries of the Financial Intelligence Unit or, in accordance with legislation, those of other supervisory authorities, investigative bodies or courts, inter alia, regarding whether the obliged entity has or has had in the preceding five years a business relationship with the given person and what is or was the nature of the relationship.

(5) Where the obliged entity makes, for the purpose of identifying a person, an enquiry with a database that is part of the state information system, the duties provided for in this subsection will be deemed performed where information on the making of an electronic enquiry to the register is reproducible over a period of five years after termination of the business relationship or making of the transaction.

(6) Upon implementation of § 31 of this Act, the obliged entity retains the data of the document prescribed for the digital identification of a person, information on making an electronic enquiry to the identity documents database, and the audio and video recording of the procedure of identifying the person and verifying the person’s identity for at least five years after termination of the business relationship.

(7) The obliged entity deletes the data retained on the basis of this section after the expiry of the time limits specified in subsections 1–6 of this section, unless the legislation regulating the relevant field establishes a different procedure. On the basis of a precept of the competent supervisory authority, data of importance for prevention, detection or investigation of money laundering or terrorist financing may be retained for a longer period, but not for more than five years after the expiry of the first time limit.

§ 48. Protection of personal data

(1) The obliged entity implements all rules of protection of personal data upon application of the requirements arising from this Act, unless otherwise provided by this Act.
[RT I, 13.03.2019, 2 - entry into force 15.03.2019]

(2) The obliged entity is allowed to process personal data gathered upon implementation of this Act only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

(3) The obliged entity submits information concerning the processing of personal data before establishing a business relationship or making an occasional transaction with them. General information on the duties and obligations of the obliged entity upon processing personal data for AML/CFT purposes is given among this information.

Chapter 5
CONDUCT IN CASE OF SUSPICION OF MONEY LAUNDERING AND TERRORIST FINANCING

§ 49. Duty to report in case of suspicion of money laundering and terrorist financing

(1) Where the obliged entity identifies in economic or professional activities, a professional act or provision of a professional service an activity or facts whose characteristics refer to the use of criminal proceeds or terrorist financing or to the commission of related offences or an attempt thereof or with regard to which the obliged entity suspects or knows that it constitutes money laundering or terrorist financing or the commission of related offences, the obliged entity must report it to the Financial Intelligence Unit immediately, but not later than within two working days after identifying the activity or facts or after getting the suspicion.

(2) Subsection 1 of this section is applied also where a business relationship cannot be established, a transaction or operation cannot be made or a service cannot be provided, and upon occurrence of the circumstances specified in §§ 42 and 43 of this Act.

(3) The obliged entity, except for a credit institution, immediately but not later than two working days after the making of the transaction, notifies the Financial Intelligence Unit of each learned transaction whereby a pecuniary obligation of over 32 000 euros or an equal sum in another currency is performed in cash, regardless of whether the transaction is made in a single payment or in several linked payments over a period of up to one year. The credit institution notifies the Financial Intelligence Unit immediately, but not later than two working days after the making of the transaction about each foreign exchange transaction of over 32 000 euros made in cash where the credit institution does not have a business relationship with the person participating in the transaction.

(4) The obliged entity immediately submits to the Financial Intelligence Unit all the information available to the obliged entity, which the Financial Intelligence Unit requested in its enquiry.

(5) The duty to report, which arises from subsections 1–4 of this section, does not apply to a notary, enforcement officer, bankruptcy trustee, auditor, attorney or other legal service provider, provider of accounting services or provider of advisory services in the field of accounting or taxation where they assess the customer's legal situation, defend to represent the customer in court, intra-authority or other such proceedings, including where they advise the customer in a matter of initiation or prevention of proceedings, regardless of whether the information has been obtained before, during or after the proceedings.

(6) Where the obliged entity suspects or knows that terrorist financing or money laundering or related criminal offences are being committed, the making of the transaction or professional act or the provision of the official service must be postponed until the submission of a report based on subsection 1 of this section. Where the postponement of the transaction may cause considerable harm, it is not possible to omit the transaction or it may impede catching the person who committed possible money laundering or terrorist financing, the transaction or professional act will be carried out or the official service will be provided and a report will be submitted the Financial Intelligence Unit thereafter.

(7) Where relevant, the Financial Intelligence Unit gives obliged entities feedback on their performance of the duty to report and on the use of the received information.

§ 50. Place and form of performance of duty to report

(1) A report is submitted to the Financial Intelligence Unit of the contracting state of the European Economic Area on whose territory the obliged entity was established, is seated or provides the service.

(2) A report is submitted via the online form of the Financial Intelligence Unit or via the X-road service.

(3) The data used for identifying the person and verifying the submitted information and, if any, copies of the documents are added to the report.

(4) Requirements for the contents and form of a notice submitted to the Financial Intelligence Unit and the guidelines for the submission of a report are established by a regulation of the minister responsible for the field.

§ 51. Confidentiality of report

(1) The obliged entity, a structural unit of the obliged legal entity, a member of a management body and an employee is prohibited to inform a person, its beneficial owner, representative or third party about a report submitted on them to the Financial Intelligence Unit, a plan to submit such a report or the occurrence of reporting as well as about a precept made by the Financial Intelligence Unit based on §§ 57 and 58 of this Act or about the commencement of criminal proceedings. After a precept made by the Financial Intelligence Unit has been complied with, the obliged entity may inform a person that the Financial Intelligence Unit has restricted the use of the person's account or that another restriction has been imposed.

(2) The prohibition provided for in subsection 1 of this section is not applied upon submission of information to:
1) competent supervisory authorities and law enforcement agencies;
2) credit institutions and financial institutions in between themselves where they are part of the same group;
3) institutions and branches that are part of the same group as the person specified in subsection 2 of this section where the group applies group-wide procedural rules and principles in accordance with § 15 of this Act;
4) a third party who operates in the same legal person or structure as an obliged entity who is a notary, enforcement officer, bankruptcy trustee, auditor, attorney or other legal service provider, provider of accounting services or provider of advisory services in the field of accounting or taxation and whereby the legal person or structure has the same owners and management system where joint compliance is practiced.

(3) The prohibition provided for in subsection 1 of this section does not apply to the exchange of information in a situation where it concerns the same person and the same transaction that involves two or more obliged entities that are credit institutions, financial institutions, enforcement officers, bankruptcy trustees, auditors, attorneys or other legal service providers, providers of accounting services or providers of advisory services in the field of accounting or taxation located in a contracting state of the European Economic Area or in a country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council are in force, act in the same field of profession and requirements equal to those in force in Estonia are implemented for keeping their professional secrets and protecting personal data.

(4) Where a notary, enforcement officer, bankruptcy trustee, auditor, attorney or other legal service provider, provider of accounting services or provider of advisory services in the field of accounting or taxation convinces a customer to refrain from unlawful acts, it is not deemed violation of the prohibition provided for in subsection 1 of this section.

(5) For AML/CFT purposes, credit institutions and financial institutions may between themselves exchange information on high-risk customers and transactions suspected of a criminal offence.

(6) The exchange of information regulated in this section must be retained in writing or in a form reproducible in writing for the next five years and information is submitted to the competent supervisory authority at its request.

§ 52. Discharge of liability

(1) The obliged entity, its employee, representative and the person who acted on its behalf is not liable for damage caused to a person or customer participating in a transaction made in economic or professional activities, in performing a professional act or in the provision of a professional service:
1) upon performance of duties and obligations arising from this Act in good faith, from failing to make the transaction or from failing to make the transaction within the prescribed time limit;
2) in connection with the performance of the duty to report provided for in § 49 of this Act in good faith;
3) by implementing §§ 16 and 18 of this Act in good faith.

(2) The performance of the duty to report arising from § 49 of this Act and submission of information by the obliged entity is not deemed breach of the confidentiality requirement arising from law or contract and the statutory or contractual liability for the disclosure of the information is not applied to the person who performed the duty to report. An agreement derogating from this provision is void.

(3) Upon releasing to the Financial Intelligence Unit data and documents relating to the professional activities of a notary on the basis of a precept of the Financial Intelligence Unit specified in § 55 of this Act or upon performance of the duty to report specified in § 49, the notary is discharged from the confidentiality duty provided for in § 3 of the Notaries Act.

(4) The obliged entity establishes a system of measures ensuring that the employees and representatives of the obliged entity who report of a suspicion of money laundering or terrorist financing either within the obliged entity or directly to the Financial Intelligence Unit are protected from being exposed to threats or hostile action by other employees, management body members or customers of the obliged entity, in particular from adverse or discriminatory employment actions.

Chapter 6

FINANCIAL INTELLIGENCE UNIT

§ 53. Financial Intelligence Unit

(1) The Financial Intelligence Unit is an independent structural unit of the Police and Border Guard Board. The Financial Intelligence Unit performs its duties arising from this Act independently and makes decisions concerning the actions provided for in this Act independently.

(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 for a term of five years.

(3) The Police and Border Guard Board ensures the provision of the Financial Intelligence Unit with funds, technical equipment and staff required for performance of the duties prescribed by law.

§ 54. Duties of Financial Intelligence Unit

(1) The duties of the Financial Intelligence Unit:
1) gathering, registration, processing and analysis of information referring to money laundering and terrorist financing;
2) strategic analysis that covers the risks, threats, trends and ways of operation of money laundering and terrorist financing;
3) tracing criminal proceeds and application of the enforcement powers of the state on the grounds and within the scope provided by law;
4) supervision over the activities of obliged entities in complying with this Act, unless otherwise provided by law;
5) informing the public about the prevention and identification of money laundering and terrorist financing, and preparing and publishing an aggregate overview at least once a year;
6) AML/CFT cooperation with obliged entities, competent supervisory authorities and investigative bodies;
7) training obliged entities' staff, investigative bodies, prosecutors and judges in AML/CFT matters;
8) organisation of international communication and exchange of information in accordance with § 63 of this Act;
9) performance of duties arising from the International Sanctions Act;
10) conducting misdemeanour proceedings provided for in this Act;
11) processing applications for authorisations, suspending or prohibiting business activities or suspending or revoking an authorisation in accordance with the procedure set out in the General Part of the Economic Activities Code Act, taking account of the variations of this Act.

(2) Upon application of clause 1 of subsection 1 of this section, it is verified whether the data submitted to the Financial Intelligence Unit is important for countering, identifying or pre-litigation investigation of money laundering, related criminal offences and terrorist financing.

(3) The Financial Intelligence Units analyses and verifies information about suspicions of money laundering and terrorist financing, takes measures for preservation of property where necessary and immediately forwards materials to the competent authorities upon identification of elements of a criminal offence. The competent authority immediately notifies the Financial Intelligence Unit of the seizure, non-seizure and release of seized property in accordance with the procedure established in the Code of Criminal Procedure.

§ 55. Administrative decisions of Financial Intelligence Unit

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

(2) A precept made on the basis of § 57 of this Act, which is aimed at stopping a transaction or restricting the use of an account or other property as well as a precept aimed at obtaining information on circumstances, transactions and persons related to a suspicion of money laundering or terrorist financing does not set out its factual grounds. The facts on the basis of which the precept is issued are set out in a separate document.

(3) The person whose transaction was stopped or the use of whose account or other property was restricted by a precept has the right to examine the document setting out the facts. The Financial Intelligence Unit has the right to refuse to grant access to the document where:
1) it would impede AML/CFT efforts;
2) the disclosure of the information contained in the document is against the law or international agreements, including restrictions established in international cooperation;
3) it would jeopardise the establishment of the truth in criminal proceedings.

(4) 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 accessed are indicated next to the signature.

(5) A claim against an administrative decision or step of the Financial Intelligence Unit is filed with the administrative court. Upon contesting a precept specified in subsection 2 of this section, the Financial Intelligence Unit submits to the administrative court a separate document setting out the facts, which gives the reasons for making the precept, establishing relevant restrictions thereto.

§ 56. Guidelines of Financial Intelligence Unit

(1) The Financial Intelligence Unit has the right to issue advisory guidelines to explain AML/CFT legislation.

(2) The Financial Intelligence Unit issues guidelines regarding the characteristics of suspicious transactions.

(3) The Financial Intelligence Unit issues guidelines regarding the characteristics of transactions suspected of terrorist financing. The guidelines are coordinated with the Estonian Internal Security Service beforehand.

(4) The guidelines of the Financial Intelligence Unit are published on its website.

§ 57. Stopping 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 stop a criminal activity or, at the request of the financial intelligence unit of another country, to suspend a transaction or impose restrictions on the disposal of property on an account, property kept on an account or property constituting the object of the transaction, professional act or professional service or other property suspected of being associated with money laundering or terrorist financing for up to 30 calendar days as of the delivery of the precept. In the event property registered in the land register, ship register, central securities depository, motor register, register of construction works 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 calendar days.

(2) Before expiry of the period specified in subsection 1, a transaction may be made or the restriction of disposal of an account or other property may be derogated from only with the written consent of the Financial Intelligence Unit.

(3) On the basis of a precept, the Financial Intelligence Unit may, in addition to the period specified in subsection 1 of this section, restrict the disposal of property for the purpose of ensuring its preservation for additional 60 calendar days where:
1) upon verification of the origin of the property in the event of suspicion of money laundering, the possessor or owner of the property fails to prove to the Financial Intelligence Unit the legal origin of the property within 30 calendar days following the suspension of the transaction or the establishment of the restriction on use of the account or on disposal of other property;
2) there is suspicion that the property is used for terrorist financing.

(4) In enforcement or bankruptcy proceedings it is prohibited to seize or transfer property on which a restriction has been imposed by the Financial Intelligence Unit in accordance with the procedure established in this section.

(5) Where property has been seized in accordance with the Code of Criminal Procedure, the Financial Intelligence Unit is required to immediately lift the restrictions on the disposal of the property after a court order on the seizure of the property has entered into force.

(6) Where the owner of the property or, in the event of property held on the account, also the beneficial owner of the property has not been established, the Financial Intelligence Unit may ask the administrative court for permission to restrict the disposal of the property until the owner or beneficial owner of the property has been established and the Financial Intelligence Unit may ask the same also upon termination of criminal proceedings, but not for more than one year.

(7) Where, within one year following the imposing of restrictions on the use of the property, the owner of the property or the beneficial owner of the property held on the account has not been identified or where the possessor of the property informs the Financial Intelligence Unit or the Prosecutor’s Office of the desire to give up the property, the Financial Intelligence Unit or the Prosecutor’s Office may ask the administrative court for permission to transfer the property to state ownership. The property is sold in accordance with the procedure provided for in the Code of Enforcement Procedure and the sum earned from the sale is transferred to state revenue. The owner of the property has the right to recover the sum transferred to the state revenue within a period of three years following the day on which the property was transferred to the state revenue.

(8) In the case of property held on an account, the account holder is deemed to be the possessor of the property upon implementation of subsections 6 and 7 of this section and their right of ownership is not presumed.

(9) The restriction of the disposal of property registered in the land register, ship register, central securities depository, motor register, register of construction works and in other state register is ensured by the registrars in the first order of priority and immediately, without any additional steps taken by the Financial Intelligence Unit.

(10) Where the legal origin of the property in the case of suspicion of money laundering or the absence of a link between the property and terrorist financing in the case of suspicion of terrorist financing is proven before the expiry of the time limit specified in subsection 1, 3 or 6 of this section, the Financial Intelligence Unit will be required to immediately terminate the restrictions of use of the property.

§ 58. Requesting information

(1) To perform the duties arising from law, the Financial Intelligence Unit has the right to receive information from the competent supervisory authorities, other state authorities and local authority agencies and, based on a precept, from obliged entities and third parties.

(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, within the time limit set in the precept. The information is submitted in writing or in a form reproducible in writing.

(3) To prevent money laundering, the Financial Intelligence Unit has the right to, in accordance with the procedure provided by law, obtain relevant information, including information collected by surveillance, from any surveillance agency. Where the Financial Intelligence Unit wishes to forward information collected by surveillance to other authorities, the Financial Intelligence Unit must obtain written consent from the agency which provided the information.

(4) This section does not apply to an attorney, unless the attorney provides the services specified in subsection 2 of § 2 of this Act or a report given by the attorney to the Financial Intelligence Unit does not meet the established requirements, is not accompanied by the required documents or is accompanied by documents that do not meet the requirements.

§ 59. Interbase cross-usage of data

In order to perform the duties 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 law.

§ 60. Restrictions on use of data

(1) Only an official of the Financial Intelligence Unit has access to and the right to process the information in the Financial Intelligence Unit database. On the basis of this Act, the head of the Financial Intelligence Unit may establish restrictions on access to information, classifying information as information for internal use. The staff of the Financial Intelligence Unit and other persons who have access to the information contained in the database of the Financial Intelligence Unit are required to keep information known to them about money laundering or terrorist financing confidential for an unspecified period of time.

(2) To prevent or identify money laundering or terrorist financing or criminal offences related thereto and to facilitate pre-litigation investigation thereof, the Financial Intelligence Unit must forward significant information, including information subject to tax and banking secrecy to the Prosecutor’s Office, the investigative body and the court.

(3) Data registered in the Financial Intelligence Unit is only forwarded to the authority engaged in the pre-litigation proceedings, the prosecutor and the court in connection with criminal proceedings or on the initiative of the Financial Intelligence Unit where it is necessary for the prevention, identification and investigation of money laundering or terrorist financing and criminal offences relating thereto as well as in administrative court proceedings where a request of the Financial Intelligence Unit or a claim or protest filed against a step or administrative decision of the Financial Intelligence Unit is decided.

(4) The Financial Intelligence Unit may notify the competent supervisory authority of the breach of the requirements of this Act by an obliged entity or, based on a relevant request, forward data registered in the Financial Intelligence Unit, analyses and assessments to the extent that does not violate restrictions established by law, an international agreement or in international cooperation, where it is necessary for AML/CFT or related criminal offences, performance of the statutory duties of the competent supervisory authority or attainment of the purposes of this Act.

(5) The Financial Intelligence Unit has the right to forward the information specified in subsection 4 of this section to the Tax and Customs Board for proceedings related to a gambling activity licence.

(6) With the permission of the head of the Financial Intelligence Unit persons whose involvement is required to perform the duties of the Financial Intelligence Unit may be granted temporary access to data required for performing the duty to the sufficient extent. The provisions of subsections 1–5 of this section and § 61 of this Act applicable to an official of the Financial Intelligence Unit apply to the rights and competences of a person who has obtained the permission.

(7) In an individual case, the Financial Intelligence Unit may forward to the compliance officer of the obliged entity the data registered in the Financial Intelligence Unit to the required and sufficient extent for the purpose of taking joint AML/CFT measures or measures for prevention of related criminal offences.

(8) The Financial Intelligence Unit has the right to establish restrictions on the use of forwarded data and the user of the data must follow the restrictions.

(9) The documents and records of the Financial Intelligence Unit, which are to be handed over to the National Archives in accordance with the law, are handed over after the passing of 30 years and thereafter the documents and records will be deleted from the database of the Financial Intelligence Unit. Until handing over to the National Archives, documents and records are kept in the Financial Intelligence Unit.

(10) The procedure for registration and processing of data gathered by the Financial Intelligence Unit is established by a regulation of the minister responsible for the field.

§ 61. Requirements for official of Financial Intelligence Unit

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

(2) An official of the Financial Intelligence Unit is required to maintain the confidentiality of information made known to them in connection with 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.

§ 62. Cooperation between Financial Intelligence Unit and Internal Security Service

(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 compliance officer who has the right to receive information of any and all reports of suspicion of terrorist financing equally to an official of the Financial Intelligence Unit and to make proposals for requesting additional information, where necessary.

(3) The compliance officer of the Internal Security Service is involved in performing the duties provided for in clauses 1, 4, 6 and 7 of subsection 1 of § 54 of this Act and their rights and competence are regulated by the provisions of subsections 1–5 of § 60 and § 61 of this Act, which are applicable to an official of the Financial Intelligence Unit.

(4) The compliance officer of the Internal Security Service has the right to exercise the supervision provided for in this Act jointly with an official of the Financial Intelligence Unit.

§ 63. International exchange of information

(1) The Financial Intelligence Unit has the right to exchange information and conclude cooperation agreements with a foreign authority that performs the duties of a financial intelligence unit (hereinafter *other financial intelligence unit*) or a foreign law enforcement agency.

(2) The Financial Intelligence Unit has the right, on its own initiative or at request, to send and receive to and from another financial intelligence unit any information that the other financial intelligence unit may need in AML/CFT efforts and in processing or analysing information relating to natural or legal persons involved in money laundering or terrorist financing.

(3) A request for information sent to a foreign financial intelligence unit by the Financial Intelligence Unit contains the circumstances of requesting the information, a description of the background, the reasons for the request and information on how they intend to use the requested information.

(4) Upon implementation of subsections 2 and 3 of this section, the Financial Intelligence Unit may use secure communication channels.

(5) When the Financial Intelligence Unit receives a report on persons and connections of another contracting state of the European Economic Area on the basis of subsections 1 and 2 of § 49 of this Act, the Financial Intelligence Unit immediately forwards the information thereon to the financial intelligence unit of the respective contracting state.

(6) When exchanging the information provided for in this section, the Financial Information Unit may, upon communication of information, establish restrictions on and conditions of the use of information and the recipient of the information must follow the established restrictions.

(7) The Financial Intelligence Union may refuse to exchange information only in exceptional cases where the exchange of information is clearly outside the aims of AML/CFT, might harm criminal proceedings, clearly and disproportionately harms the legitimate interests of a natural or legal person or the Financial Intelligence Unit, is otherwise in conflict with the general principles of national law or does not contain the circumstances of requesting the information, a description of the background, the reasons for the request or information on how the requested information is to be used.

(8) The Financial Intelligence Unit ensures the use of information received from another financial intelligence unit on the basis of a request in accordance with the restrictions established by the other unit, asking for the other unit's prior consent to using the information in another manner, where necessary.

(9) The Financial Intelligence Unit ensures that the consent to disseminate the information communicated based on a request is granted immediately and to the highest extent possible. The Financial Intelligence Unit that has received a request may refuse to grant consent to the dissemination of the information to the requested extent where it is clearly outside the aims of AML/CFT, might harm criminal proceedings, clearly and disproportionately harms the legitimate interests of a natural or legal person or the Financial Intelligence Unit or is otherwise in conflict with the general principles of national law. The restriction of dissemination of information is explained.

Chapter 7
SUPERVISION

§ 64. Supervisory authorities

(1) The Police and Border Guard Board or the Financial Intelligence Unit exercises state supervision over compliance with this Act and legislation adopted on the basis thereof, unless otherwise provided for in this section.

(2) The Financial Supervision Authority exercises supervision over compliance with this Act and legislation adopted on the basis thereof by credit institutions and financial institutions that are subject to its supervision under the Financial Supervision Authority Act and in accordance with the legislation of the European Union. The Financial Supervision Authority exercises supervision in accordance with the procedure provided for in the Financial Supervision Authority Act, taking account of the variations provided for in this Act. The Financial Supervision Authority exercises supervision over the credit institutions and financial institutions specified in the first sentence of this subsection in all the fields of activity specified in § 2 of this Act and in the provision of the services specified in § 6.

(3) The board of the Estonian Bar Association (hereinafter *Bar Association*) exercises supervision over compliance with 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 account of the provisions of this Act.

(4) The Ministry of Justice exercises supervision over compliance with this Act and legislation adopted on the basis thereof by notaries on the basis of the Notaries Act, taking account of the provisions of this Act. 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 based on the purposes of this Act.

(6) The supervisory authorities have the right to exchange information and cooperate with the supervisory authorities of other countries based on the duties provided for in this Act.

(7) A supervisory authority has the right to involve experts, interpreters and advisors in exercising supervision, provided that the compliance of such person with the requirements specified in subsection 1 of § 61 of this Act is ensured.

§ 65. Application of state supervisory measures and imposition of penalty payment

(1) To exercise state supervision provided for in this Act, the Police and Border Guard Board and the Financial Intelligence Unit may apply the special measures of state supervision provided for in §§ 30–32, 35, 50 and 51 of the Law Enforcement Act, taking account of the variations provided for in this Act and in the Financial Supervision Authority Act.

(2) Where the obliged entity is a credit institution or financial institution, the maximum penalty payment in the event of failure to comply or improper compliance with an administrative decision is:
1) in the case of a natural person, up to 5000 euros the first time and up to 50 000 euros any next time in order to force the person to perform one and the same duty or obligation, but not more than 5 000 000 euros in total;
2) in the case of a legal person, up to 32 000 euros the first time and up to 100 000 euros any next time in order to force the person to perform one and the same duty or obligation, but not more than the higher of 5 000 000 euros or 10 per cent of the total annual turnover of the legal person according to the latest available annual accounts approved by its management body.

(3) Where the legal person specified in clause 2 of subsection 2 of this section is a parent undertaking or a subsidiary of such parent undertaking who must prepare consolidated annual accounts, either the annual turnover or the total turnover of the field of the breach that served as the basis for the given administrative decision or precept according to the latest available consolidated annual accounts approved by the highest-level management body of the parent undertaking is considered the legal person's total annual turnover.

(4) In the case of obliged entities not specified in subsection 3 of this section, the maximum penalty payment is equal to up to twice the profit earned as a result of the breach, where such profit can be determined, or at least 1 000 000 euros.

§ 66. Rights of administrative supervision authority

(1) The administrative supervision authority has the right to inspect the seat or the place of business of obliged entities. The supervisory authority has the right to enter a building and a room that is in the possession of the obliged entity in the presence of a representative of the inspected person.

(2) In the event of on-site inspection, the administrative supervision authority has the right to:
1) without limitations examine the required documents and data media, make extracts, transcripts and copies thereof, receive explanations regarding them from the obliged entity, and monitor the work processes;
2) receive oral and written explanations from the inspected obliged entity, members of its management body and employees.

(3) The administrative supervision authority has the right to demand that an obliged entity submit information required for inspection also without carrying out an on-site inspection.

§ 67. Duties of supervisory authority

(1) Where the Financial Supervision Authority, the Police and Border Guard Board, the board of the Bar Association, the Ministry of Justice or the Chamber of Notaries, upon exercising supervision, identifies a situation whose characteristics refer to a suspicion of money laundering or terrorist financing, it will immediate notify the Financial Intelligence Unit thereof based on § 49 of this Act.

(2) The Financial Supervision Authority, the board of the Bar Association and the Ministry of Justice must submit to the Financial Intelligence Unit by 15 April information about:
1) the number of supervisory proceedings carried out in the preceding calendar year and the number of obliged entities covered by supervision based on the types of entities;
2) the number of breaches detected upon exercising supervision in the preceding calendar year, the number of persons against whom misdemeanour proceedings were initiated or other measures were applied, and the legal grounds per obliged entity.

(3) The Police and Border Guard Board, the Financial Intelligence Unit and the Financial Supervision Authority publish on their websites the final decision made in a misdemeanour case provided for in Chapter 10 of this Act or an administrative decision, precept or decision to impose a penalty payment made in accordance with the procedure established in this Chapter immediately after it has entered into force. At least the type and nature of the breach, the details of the person responsible for the breach and information on appealing against and annulment of the decision or precept is given on the website. The entire information must remain available on the website for at least five years.

(4) Upon assessment of the facts, the Police and Border Guard Board, the Financial Intelligence Unit and the Financial Supervision Authority has the right to postpone the publication of the final decision in a misdemeanour case or a relevant administrative decision or not to disclose the identity of the offender for the purpose of protection of personal data as long as at least one of the following criteria is met:
1) the publication of the data jeopardises the stability of financial markets or pending proceedings;
2) the disclosure of the person responsible for the misdemeanour would be disproportionate to the imposed penalty.

(5) Upon assessment of the facts, the Police and Border Guard Board, the Financial Intelligence Unit and the Financial Supervision Authority has the right not to publish the final decision made in the misdemeanour case or the relevant administrative decision where the options specified in subsection 4 of this section are deemed insufficient to ensure the stability of financial markets or the publishing of the decisions would be disproportionate in the case of a measure considered less important.

§ 68. Reporting of inspection results

(1) The Financial Supervision Authority must prepare a report on the inspection results, which is communicated to the inspected person within the time limit provided for in the Act regulating the activities of the credit institution or financial institution. Another administrative supervision authority must prepare a report on the inspection results, which is communicated to the inspected person within one month after the inspection.

(2) The report must contain the following details:
1) the name of the inspection;
2) the job title and given name and surname of the author of the inspection report;
3) the place and date of preparation of the report;
4) reference to the provision serving as the basis for the inspection;
5) the given name and surname and the job title of the representative of the inspected person or the possessor of the building or room who attended the inspection;
6) the given name and surname and the job title of another person who attended the inspection;
7) the start and end time and the conditions of the inspection;
8) the process and results of the inspection with the required level of detail.

(3) The report is signed by its author. The report remains with the administrative supervision authority and a copy thereof to the inspected person or its representative.

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

§ 69. 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) To assess the Financial Intelligence Unit's personal data processing process, the Data Protection Inspectorate has the right to access the guidelines and procedures of the Financial Intelligence Unit and receive written and oral clarifications. In the course of deciding a complaint filed by a data subject, the Data Protection Inspectorate has the right to receive data from the Financial Intelligence Unit to the extent required for making a decision on the complaint.

(3) Supervisory control over the lawfulness of the activities of the Financial Intelligence Unit is exercised by the Police and Border Guard Board.

(4) The Director General of the Police and Border Guard Board and an official authorised by them has the right to access data registered in the Financial Intelligence Unit for the purpose of exercising supervisory control to the required extent.

(5) The provisions of subsections 1–5 of § 60 and § 61 of this Act regarding an official of the Financial Intelligence Unit apply to an official exercising supervisory control.

Chapter 8
AUTHORISATION

§ 70. 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 pawnbroking services;
4) providing services of exchanging a virtual currency against a fiat currency;
5) providing a virtual currency wallet service;
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) A person who holds the following is not subject to the authorisation obligation:
1) authorisation granted by the Financial Supervision Authority;
2) obligation to apply for the Financial Supervision Authority's authorisation under another Act;
3) authorisation granted by the financial supervision authority of a contracting state of the European Economic Area 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, or
4) who provides the services specified in subsection 1 of this section within the group.

(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) where the undertaking that is a legal person has not been registered in the Estonian commercial register: the name of the owner of the undertaking, the owner's registry code or personal identification code (upon absence thereof, the date of birth), the seat or place of residence; the beneficial owner's name, personal identification code (upon absence thereof, the date of birth), the place of birth, and the address of the place of residence;
4) the name, personal identification code (upon absence thereof, the date of birth), place of birth and the address of the place of residence of a member of the management 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;
5) the rules of procedure and internal control rules drawn up in accordance with §§ 14 and 15 of this Act and, in the case of persons having specific duties listed in § 6 of International Sanctions Act, the rules of procedure and the procedure for verifying adherence thereto drawn up in accordance with subsection 6 of § 12 of the International Sanctions Act;
6) the name, personal identification code (upon absence thereof, the date of birth), place of birth, citizenship, address of the place of residence, position, and contact details of the compliance officer appointed in accordance with § 17 of this 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 person who is in charge of imposing the international financial sanction and who has been appointed by the undertaking in accordance with subsection 6 of § 12 of the International Sanctions Act;
8) where the undertaking, a member of its management body, procurator, beneficial owner or owner is a foreign national or where the undertaking is a foreign service provider, a certificate of the criminal records database 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 authenticated by a notary or certified in accordance with an equivalent procedure and legalised or certified with a certificate replacing legalisation (apostille), unless otherwise provided by an international agreement.

(4) In the case of an application for authorisation in a field specified in clause 1 of subsection 1 of this section, the details specified in subsection 3 of this section must be accompanied by information on which financial service will be provided.

(5) Where the undertaking would like to use the authorisation also for the activities of a 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 3 of this section and, where necessary, also the information specified in subsection 4 of this section.

§ 71. Applying for authorisation

An authorisation application is decided by the Financial Intelligence Unit by way of granting or refusing to grant authorisation not later than within 30 working days following the date of submission of the application.

§ 72. Object of inspection of authorisation

Authorisation will be granted to an undertaking where:
1) the undertaking, a member of its management body, procurator, beneficial owner and owner do 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 § 17 of this Act meets the requirements provided for in this Act;
3) the undertaking's subsidiary for whose activities the authorisation to be applied in the name of the undertaking is to be used meets the requirements specified in clauses 1 and 2 of this section.

§ 73. Obligation to enclose documents with notice of intention to change business activity

Where an undertaking submits a notice of intention to change its business activity regarding itself, a member of its management body, procurator, beneficial owner or owner, the document specified in clause 8 of subsection 3 of § 70 of this Act must be enclosed with the notice where the undertaking is a foreign service provider or the member of its management body, procurator, beneficial owner or owner is a foreign national.

§ 74. Obligation to notify of change of circumstances relating to business activities

In a notice of the intention to change the business activity and in a notice of the change of the business activity the undertaking describes 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 submits, regarding its subsidiary that will commence economic activities within the object of regulation of the

authorisation, all the information specified in subsection 3 of § 70 of this Act and the information specified in clauses 1–3, 5 and 6 of subsection 1 of § 14 of the General Part of the Economic Activities Code Act.

§ 75. Revocation of authorisation

In addition to the grounds provided for in subsection 1 of § 37 of the General Part of the Economic Activities Code Act, the Financial Intelligence Unit will revoke authorisation specified in subsection 1 of § 70 of this Act where:
1) the Financial Supervision Authority has granted authorisation to the undertaking;
2) the undertaking repeatedly fails to follow the precepts of the supervisory authority;
3) the undertaking has not commenced operation in the requested field of activity within six months from the issue of the authorisation.

Chapter 9
DATA OF BENEFICIAL OWNER OF LEGAL PERSON AND LIABILITY ACCOUNT

§ 76. Duty to keep data of beneficial owner

(1) A legal person in private law gathers and retains data on its beneficial owner, including information on its right of ownership or manners of exercising control. The data of the beneficial owner is kept in the commercial register by the management board of the private legal person.

(2) To enable the performance of the duty specified in subsection 1 of this section, the shareholders or members of a private legal person must provide the management board of the legal person with all the information known to them about the beneficial owner, including information on its right of ownership or manners of exercising control.

(3) The duty specified in subsection 1 of this section does not apply to:
1) an apartment association provided for in the Apartment Ownership and Apartment Associations Act;
[RT I, 17.11.2017, 2 - entry into force 01.01.2018]
2) a building association provided for in the Building Association Act.
3) a company listed on a regulated market;
4) a foundation provided for in the Foundations Act the purpose of whose economic activities is the keeping or accumulating of the property of the beneficiaries or the circle of beneficiaries specified in the articles of association and who has no other economic activities.

§ 77. Submission of data

(1) Based on subsections 2–4 of § 9 and § 76 of this Act, a general partnership, limited partnership, private limited company, public limited company or commercial association submits via the commercial register information system the following data on its beneficial owner:
1) the person's name, personal identification code and the country of the personal identification code (upon absence of a personal identification code, the date and place of birth), and the country of residence;
2) nature of the beneficial interest held.

(2) Based on subsection 7 of § 9 of this Act, a non-profit association submits via the commercial register information system the following data on its beneficial owner:
1) the person's name, personal identification code and the country of the personal identification code (upon absence of a personal identification code, the date and place of birth), and the country of residence;
2) nature of the beneficial interest held.

(3) Based on subsection 7 of § 9 of this Act, a foundation submits via the commercial register information system the following data on its beneficial owner:
1) the person's name, personal identification code and the country of the personal identification code (upon absence of a personal identification code, the date and place of birth), and the country of residence;
2) nature of the beneficial interest held;
3) the list of beneficiaries within the meaning of § 9 of the Foundations Act, which contains each beneficiary's name, personal identification code and the country of the personal identification code (upon absence of a personal identification code, the date and place of birth), and the country of residence, where such persons have been specified in the articles of association of the foundation.

(4) A company, non-profit association or foundation must submit the data of the beneficial owner along with the application for registration in the commercial register.

(5) Where the submitted data changes, the company, non-profit association or foundation submits new data via the commercial register information system not later than within 30 days after learning of the changes in the data.

(6) Where the data of the beneficial owner has not changed, the company, non-profit association or foundation certifies the correctness of the data upon submission of the annual report.

§ 78. Publication of data

(1) The data of the beneficial owner are made public in the commercial register information system.

(2) The fees for issuing the data of a beneficial owner are established by a regulation of the minister responsible for the field.

(3) The data of the beneficial owner is issued free of charge to the obliged entity, a government agency, the Financial Supervision Authority and to a court.

§ 79. Beneficial owner's right to demand correction of submitted data

(1) The person indicated as the beneficial owner or their legal or contractual representative has the right to request that the management board of the legal person correct incorrect data.

(2) Where the management board of the legal person has without reason refused to correct the incorrect data as requested on the basis of subsection 1 of this section, the person indicated as the beneficial owner may demand that the legal person compensate for damage caused by making incorrect data public.

§ 80. Deletion of data

The data of the beneficial owner is deleted automatically five years after deleting the legal person from the register.

§ 81. Mandatoriness of automated communication of liability account information

(1) A credit institution or a financial institution that has in a business relationship opened for a customer a liability account (hereinafter *account*) that has an International Bank Account Number (IBAN) must join the electronic seizure system and ensure that at least the following data is available via the system:
1) the name of the account holder and the person making transactions in the name of the account holder along with the information received upon implementation of clause 1 of subsection 1 of § 20 of this Act;
2) the data of the beneficial owner of the account holder along with the information received upon implementation of clause 3 of subsection 1 of § 20 of this Act;
3) the IBAN of the account;
4) the dates of opening and closing the account.

(2) For the purposes of this section, 'IBAN' means an International Bank Account Number that complies with the EVS 876:2016 standard and whose elements have been determined by the International Organization for Standardization and that uniquely identifies a specific account in a Member State.

(3) A credit institution and a financial institution specified in subsection 1 of this section ensure that an enquiry regarding the data specified in subsection 1 of this section, which is filed via the electronic seizure system, can be answered also over a period of five years from the date of closing the account.

Chapter 10
LIABILITY

§ 82. Giving of order not to implement money laundering and terrorist financing due diligence measures, risk assessment, procedural rules and internal control rules

(1) The penalty for giving an order by a management board member of the obliged entity not to implement due diligence measures, the risk assessment specified in § 13 of this Act, procedural rules or the internal control rules 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 400 000 euros.

§ 83. Opening of anonymous account or savings book

(1) The penalty for making a decision by an employee of a credit institution or financial institution to open an anonymous account or savings book or for concluding a respective contract 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 400 000 euros.

§ 84. Failure to perform duty to identify person and verify person's identity

(1) The penalty for a breach by an obliged entity, its management board member or employee of the duty provided for in this Act to identify and verify the identity of a customer or a person participating in an occasional transaction or the representative of a 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 400 000 euros.

§ 85. Breach of duty to identify beneficial owner

(1) The penalty for a breach by an obliged entity or its management board member or an employee of the duty provided for in this Act to identify the beneficial owner and verify their identity 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 400 000 euros.

§ 86. Breach of requirements for gathering and assessing information

(1) The penalty for a breach of the requirements for gathering information on the purpose and nature of a business relationship or an occasional transaction by an obliged entity, its management board member or employee 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 400 000 euros.

§ 87. Breach of requirements for making of transaction with politically exposed person

(1) The penalty for a breach of the requirements for making a transaction with a politically exposed person by an obliged entity, its management board member or employee 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 400 000 euros.

§ 88. Violation of prohibition to establish business relationship and make occasional transaction

(1) The penalty for violation by an obliged entity, its management board member or employee of the prohibition to establish a business relationship and make an occasional transaction 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 400 000 euros.

§ 89. Breach of duty to monitor business relationship

(1) The penalty for a breach by an obliged entity, its management board member or employee of the duty provided for in this Act to monitor a business relationship 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 400 000 euros.

§ 90. Violation of prohibition to outsource activity

(1) The penalty for outsourcing an activity by an obliged entity or its management board member to a person established in a high-risk third country 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 400 000 euros.

§ 91. Breach of correspondent banking requirements

(1) The penalty for establishing a correspondent relationship by breaching the requirements 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 400 000 euros.

§ 92. Breach of duty to report suspicion of money laundering or terrorist financing

(1) The penalty for a breach of the duty to notify the Financial Intelligence Unit of a suspicion of money laundering or terrorist financing, a foreign exchange transaction or another transaction where a pecuniary 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.

(2) The penalty for the same act committed by a legal person is a fine of up to 400 000 euros.

§ 93. Illegal notification of data forwarded to Financial Intelligence Unit

(1) The penalty for illegal notification of a person, their representative or the person's beneficial owner by the obliged entity, its management board member, compliance officer or employee or by an employee of a supervisory authority about a report or data submitted to the Financial Intelligence Unit regarding them or about a precept made by the Financial Intelligence Unit regarding them or about the commencement of criminal proceedings instituted regarding them 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 400 000 euros.

§ 94. Breach of requirement to register and retain data

(1) The penalty for a breach of the requirement to register and retain data 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 400 000 euros.

§ 95. Failure to submit data of beneficial owner or submission of false data

(1) The penalty for failure by a shareholder or member of a private legal person to submit the data of the beneficial owner or for failure to report on a change of the data or for knowingly submitting false data, where a situation where the obliged entity cannot take the due diligence measure provided for in clause 3 of subsection 1 of § 20 of this Act has been caused, 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.

§ 96. Breach of duties of payment service provider

(1) The penalty for failure by an executive or employee of a payment service provider or by an executive or employee of a paying agent or a natural person paying agent to identify, verify or information relating to a payer as well as for a breach of the duties of a payment service provider established in Regulation (EU) No 2015/847 of the European Parliament and of the Council 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 400 000 euros.

§ 97. Proceedings

Extrajudicial proceedings of misdemeanours specified in this Chapter are the Police and Border Guard Board and the Financial Supervision Authority.

Chapter 11
IMPLEMENTING PROVISIONS

§ 98. Follow-up analysis of implementation of Act

By 31 December 2018, the Ministry of Finance will analyse the practicality and purposefulness of implementation of the real-time interview requirement regarding the establishment of a business relationship and the sufficiency of the provisions regulating the submission of the information of beneficial owners and, where necessary, submit proposals for amendment of legislation to the Finance Committee of the *Riigikogu*.

§ 99. Variation of application of due diligence measures by gambling operator

Until 31 August 2018, a gambling operator applies due diligence measures at least in the case of payment of winnings, making of bets or both where the amount given or received by a customer is at least 2000 euros or an equal sum in another currency.

§ 100. Duty to re-apply provisions to existing customer relationships

Where necessary, the obliged entity applies the due diligence measures specified in Chapter 3 of this Act to the existing customers over a period of one year from the entry into force of the Act. Upon assessment of the need to apply the due diligence measures, the obliged entity relies on, inter alia, the importance of the customer and the risk profile as well as the time that has passed from the previous application of the due diligence measures or the scope of their application.

§ 101. Deadline of updating risk assessment and procedural rules

(1) The obliged entity must bring its activity into compliance with the requirements of this Act within one year as of the entry into force of this Act.

(2) A person subject to the authorisation obligation specified in subsection 1 of § 70 of this Act submits to the Police and Border Guard Board a risk assessment specified in § 13 of this Act and the corresponding rules of procedure and the internal control rules within one year from the entry into force of this Act.

§ 102. Information on existing outsourcing contract

The obliged entity submits to the competent supervisory authority informational on an outsourcing contract in force at the time of entry into force of this Act in accordance with the procedure provided for in subsection 4 of § 24 of this Act within five months from the entry into force of this Act and notifies the competent supervisory authority about amendment of the contract for the purpose of bringing it into compliance with the requirements of this Act.

§ 103. Authorisation of provider of service of alternative means of payment

(1) Within eight months following the entry into force of this Act, an undertaking holding the authorisation of a provider of a service of an alternative means of payment notifies the Police and Border Guard Board about whether it wishes to change its authorisation to that of a provider of the service of exchanging virtual currency against a fiat currency. Upon receipt of a relevant notification, the Police and Border Guard Board makes, within 30 working days following the day of submission of the application, a decision to grant the authorisation without the obligation to pay the state fee and without additionally verifying the facts falling within the object of inspection of the authorisation.

(2) The authorisation of a provider of a service of alternative means of payment becomes invalid nine months after the entry into force of this Act.

§ 104. Duty to report of legal person registered in commercial register or in register of non-profit associations and foundations

The management board of a legal person registered in the commercial register or the register of non-profit associations and foundations before the entry into force of this Act declares to the commercial register the data of the beneficial owner within 60 days following the entry into force of this provision.

§ 105. Form of performance of duty to report

Until 30 June 2018, a report specified in subsection 2 of § 50 of this Act is submitted orally, in writing or in a form reproducible in writing. Where a report was submitted orally, it will be repeated the next working day in writing or in a form reproducible in writing.

§ 106.–§ 111.[Omitted from this text.]

§ 112. Repeal of Money Laundering and Terrorist Financing Prevention Act

The Money Laundering and Terrorist Financing Prevention Act (RT I 2008, 3, 21) is repealed.

§ 113. Amendment of Money Laundering and Terrorist Financing Prevention Act

In clause 2 of subsection 9 of § 9 and in clause 1 of subsection 3 of § 76 of the Money Laundering and Terrorist Financing Prevention Act, the words ‘Apartment Association Act’ are replaced with the words ‘Apartment Ownership and Apartment Associations Act.’

§ 114.–§ 118.[Omitted from this text.]

§ 119. Entry into force of Act

(1) Subsection 3 of § 19 and §§ 76–80 of this Act enter into force on 1 September 2018.

(2) Section 113 of this Act enters into force on 1 January 2018.

(3) Sections 81 and 95 of this Act enter into force on 1 January 2019.

[1]Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 05.06.2015, pp 73–117).