Issuer:	Riigikogu
Type:	Act
In force from:	30.12.2024
In force until:	31.12.2024
Translation published:	03.12.2024

Money Laundering and Terrorist Financing Prevention Act[1]

Passed 26.10.2017
RT I, 17.11.2017, 2
Entry into force 27.11.2017, subsection 3 of § 19 and §§ 76–80 on 01.09.2018 and §§ 81 and 95 on 01.01.2019

Amended by the following acts

Passed	Published	Entry into force
26.10.2017	RT I, 17.11.2017, 2	27.11.2017, in part 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
20.02.2019	RT I, 19.03.2019, 11	01.01.2020
11.12.2019	RT I, 31.12.2019, 2	10.03.2020
17.06.2020	RT I, 10.07.2020, 1	20.07.2020, in part 10.09.2020, 01.01.2021, 10.01.2021 and 10.05.2021; amended in part [RT I, 21.11.2020, 1]
12.11.2020	RT I, 21.11.2020, 1	23.11.2020, in part 01.01.2021
16.12.2020	RT I, 04.01.2021, 1	01.05.2021
17.03.2021	RT I, 26.03.2021, 1	01.01.2022
24.03.2021	RT I, 09.04.2021, 1	01.01.2024
06.04.2021	RT I, 14.04.2021, 1	24.04.2021, in part 30.06.2021
12.05.2021	RT I, 02.06.2021, 1	12.06.2021, in part 07.03.2022
23.02.2022	RT I, 12.03.2022, 2	15.03.2022
13.04.2022	RT I, 05.05.2022, 1	01.02.2023
25.01.2023	RT I, 10.02.2023, 3	20.02.2023, in part 01.09.2023
22.02.2023	RT I, 17.03.2023, 2	01.11.2023
20.06.2023	RT I, 06.07.2023, 6	01.01.2024
05.06.2024	RT I, 21.06.2024, 3	01.07.2024, in part 30.12.2024 and 01.07.2026

Chapter 1
General Provisions

Subchapter 1
Purpose and Scope of Regulation

§ 1. Purpose and scope of regulation

(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;
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]
3) supervision over obliged entities in complying with this Act;
4) duties and obligations in relation to the collection and disclosure of information on beneficial owners;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
5) duties and obligations related to the collection and disclosure of information on 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 this Act

(1) This Act applies to the economic, professional and official activities of the following persons:
1) credit institutions;
2) financial institutions;
3) gambling operators, except for organisers of commercial lotteries;
4) persons that mediate the purchase or sale of an immovable;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
4^1) persons that mediate transactions of use of an immovable whereby the usage fee agreed in the transaction amounts to no less than 10,000 euros per month;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
5) traders, where a cash payment of at least 10,000 euros or an equivalent sum in another currency is made to or by the trader, regardless of whether the financial obligation is performed in the transaction as a single payment or as several related payments over a period of up to one year, unless otherwise provided for by law;
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]
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) certified auditors, upon provision of accounting services, and providers of accounting services;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
8) providers of accounting or tax advice services;
9) providers of trust and company services;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
10) providers of a virtual currency service;
[RT I, 31.12.2019, 2 – entry into force 10.03.2020
11) [Repealed – RT I, 31.12.2019, 2 – entry into force 10.03.2020]
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;
15) dealers of works of art and persons that mediate works of art or store them in a customs free zone whereby a payment of no less than 10,000 euros is made to or by them as a single payment or as several connected payments over the course of one year.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2) This Act applies to the economic, professional or official activities of notaries, attorneys, enforcement agents, 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, professional or official activities of a said person where the person guides the planning or making of a transaction or makes an official operation or provides an official 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.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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 that Act as well as to foundations for the purposes of the Foundations Act where they are paid or they pay, in cash, over 5,000 euros or an equivalent sum in another currency, regardless of whether it is paid as a single payment or as several related payments over a period of up to one year; this Act also applies where the customer or a person participating in the transaction has a connection to a State or jurisdiction that is mentioned in clause 3 of subsection 4 of § 37 of this Act.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(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 equivalent sum in another currency or where it is paid over 10,000 euros in cash or an equivalent sum in another currency for collector coins or other numismatic-bonistic products, regardless of whether it is paid as a single payment or as several related payments over a period of up to one year.

(5) The provisions of this Act governing financial institutions apply to virtual currency service providers mentioned in clause 10 of subsection 1 of this section. The application of this Act to a virtual currency service provider is based on the provider's actual intention and the nature and purpose of the provider's activity.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(6) Chapter 9 of this Act applies to all private legal persons and trustees.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

Subchapter 2
Definitions

§ 3. Definitions used in this 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 in respect of such an 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, professional or official activities while providing a service or official service, performing official operations 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;
9^1) 'virtual currency service' means a service mentioned in clauses 10–10^3 of this subsection;
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]
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;
10^1) 'virtual currency exchange service' means a service with the help of which a person exchanges a virtual currency against a fiat currency or a fiat currency against a virtual currency or a virtual currency against another virtual currency;
[RT I, 31.12.2019, 2 – entry into force 10.03.2020]
10^2) 'virtual currency transfer service' means a service that allows a transaction to be conducted electronically at least in part through the virtual currency service provider in the name of the initiating party with the aim of moving the virtual currency to the recipient's virtual currency wallet or virtual currency account, regardless of whether the initiator and the recipient are one and the same party or whether the initiator and recipient are using the same service provider;
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]
10^3) organisation, in the name or on behalf of an issuer of virtual currency, of a public or targeted offering or sale related to the issue of such currency, or the provision of any related financial services;
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]
11) [Repealed – RT I, 10.07.2020, 1 – entry into force 20.07.2020]
12) [Repealed – RT I, 10.07.2020, 1 – entry into force 20.07.2020]
13) [Repealed – RT I, 10.07.2020, 1 – entry into force 20.07.2020]
14) [Repealed – RT I, 10.07.2020, 1 – entry into force 20.07.2020]
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);
19) ‘crypto-assets’ are crypto-assets within the meaning of popint 5 of paragraph 1 of Article 3 of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (OJ L 150, 09.06.2023, pp. 40–205), except where they fall within a category mentioned in paragraphs 2–4 of Article 2, or otherwise qualify as money;
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]
20) ‘self-hosted address’ means a self-hosted address within the meaning of point 20 of Article 3 of Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (OJ L 150, 09.06.2023, pp. 1–39).
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

§ 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 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;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
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 of the true nature, origin, location, manner of disposal, relocation or right of ownership of property acquired as a result of a criminal activity or property acquired instead of such property or the concealment of other rights related to such property.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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;

3[1]) a crypto-asset service provider within the meaning of point 15 of paragraph 1 of Article 3 of Regulation (EU) 2023/1114 of the European Parliament and of the Council, who provides one or several crypto-asset services provided for by point 16 of paragraph 1 of Article 3, with the exception of persons providing the crypto-asset service mentioned at sub-point h of that point;
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]
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, which is a person specified in clauses 1–11 of this subsection.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 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 institution) to another credit institution (respondent institution), 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;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
2) relationships between and among credit institutions and financial institutions, including relationships within which similar services are provided by a correspondent institution to a respondent institution for the purpose of servicing its customers, and including relationships established for securities transactions or funds transfers, or relationships established in order to carry out transactions in or transfers of crypto-assets.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

§ 7[1]. Trust

(1) For the purposes of this Act, 'trust' means a legal relationship established on the basis of or arising from the law of the country recognising it, according to which trust property formed by a settlor is administered by a trustee in the trustee's own name but in the interests of beneficiaries or for another defined purpose, as well a legal arrangement specified in the consolidated list published the European Commission on the basis of Article 31(10) of Directive (EU) 2015/849 of the European Parliament and of the Council.

(2) The submission of information prescribed by this Act on a trust does not entail legal consequences other than those provided for in this Act.

(3) A country that recognises trusts means a country that is party to the Hague Convention of 1 July 1985 on the Law Applicable to Trusts and on their Recognition.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 8. Provider of trust and company services

[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
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:
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
1) foundation of a company or another legal person, including operations 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 trustee or a representative of a civil law partnership, community or legal arrangement, or the appointment of another person to such position;

[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
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:
1) who, via ownership or other type of control, has the final dominant influence over a natural or legal person, or
2) in whose interests, for the benefit of whom or in whose name a transaction or operation is made.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2) Where a beneficial owner cannot be identified in the manner specified in subsection 1 of this section, the beneficial owner of a company is a natural person whose direct or indirect shareholding or the total shareholding of all of the direct and indirect shareholdings in the company exceeds 25 per cent, including shareholdings in the form of bearer shares or otherwise.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(3) 'Direct shareholding' means that a natural person personally holds shares in a company. 'Indirect shareholding' means that a natural person holds shares in a company via one or multiple persons or a chain of persons.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(4) Where, after all possible means of identification have been exhausted, the person specified in subsection 1 or 2 of this section cannot be identified and there is no ground for calling the existence of such person into doubt or where there are doubts as to whether the identified person is the beneficial owner, the natural person who holds the position of a senior managing official is deemed to be the beneficial owner.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(4^1) Where several persons meet the terms provided for in subsection 4 of this section, including where there are several senior managing officials, several senior management bodies or where another legal persons holds shares in a company via one or several persons or chains of persons, the person(s) who exercise(s) actual control over the company and make(s) strategic decisions in the company or, upon absence of such persons, perform(s) day-to-day and regular management is (are) considered the beneficial owner(s).
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(4^2) Where the beneficial owner of a company is a trustee, all of the persons specified in clauses 1–5 of subsection 6 of this section are considered beneficial owners.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(5) [Repealed – RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(6) In the case of a trust or a legal arrangement, the beneficial owner is:
1) the settlor of the trust or the establisher of the arrangement;
2) the trustee;
3) the person ensuring and controlling the preservation of property, where such person has been appointed;
4) the beneficiary, or where the beneficiary or beneficiaries are yet to be determined, the class of persons in whose main interest such triste or arrangement has been set up or operates;
5) any other person who in any way exercises ultimate control over the property of the trust or arrangement.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(7) In the case of a person or an association of persons not specified in subsections 2 and 6 of this section, the members of the management board or the chairman of the management board may be designated as the beneficial owner(s), taking into account clause 1 of subsection 1.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(8) [Repealed – RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(9) [Repealed – RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 9^1. Politically exposed person

(1) A politically exposed person for the purposes of this Act means a natural person who performs or has performed prominent public functions and with regard to whom related risks remain.

(2) At least the following persons are deemed to perform prominent public functions:
1) head of State or head of government;
2) minister, deputy minister or assistant minister;
3) member of a legislative body;

4) member of a governing body of a political party;
5) judge of the highest court of a country;
6) auditor general or a member of the supervisory board or executive board of a central bank;
6[1]) the Chancellor of Justice;
[RT I, 14.04.2021, 1 – entry into force 24.04.2021]
7) ambassador, envoy or chargé d'affaires;
8) high-ranking officer in the armed forces;
9) member of an administrative, management or supervisory body of a state-owned enterprise;
10) director, deputy director and member of a management body of an international organisation.

(3) Regardless of subsection 2 of this section, middle-ranking or more junior officials are not considered politically exposed persons.

(4) A person who, as per list published by the European Commission, is considered a performer of prominent public functions by a Member State of the European Union, the European Commission or an international organisation accredited on the territory of the European Union is deemed a politically exposed person.

(5) A list of Estonian positions whose holders are considered politically exposed persons is established by a regulation of the minister in charge of the policy sector.

(6) An international organisation accredited in Estonia draws up a list of the positions of its organisation whose holders are considered politically exposed persons, keeps it up to date and informs the minister in charge of the policy sector of changes made to the list.

(7) For the purposes of this Act, 'family member' of a politically exposed person means their:
1) spouse or a person considered to be equivalent to a spouse;
1[1]) registered partner;
[RT I, 06.07.2023, 6 – entry into force 01.01.2024]
2) parent;
3) child;
4) child's spouse or a person considered to be equivalent to a spouse;
5) child's registered partner.
[RT I, 06.07.2023, 6 – entry into force 01.01.2024]

(8) For the purposes of this Act, 'person known to be close associates' of a politically exposed person means a natural person who is:
1) known to have joint beneficial ownership of a legal person or trust with a politically exposed person;
2) known to have close business relations with a politically exposed person;
3) the beneficial owner of a legal person or trust set up in the interests of a politically exposed person.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 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 are established with persons non-EEA countries.
[RT I, 10.07.2020, 1 – entry into force 10.09.2020]

Chapter 2

Management of Risks Relating to Money Laundering and Terrorist Financing

Subchapter 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;
5) reports on the institutional structure and broad procedures of the AML/CFT regime and on the human and financial resources allocated for such purpose.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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 made available to obliged entities, the European Commission, European Banking Authority and other Member States of the European Union without delay.
[RT I, 14.04.2021, 1 – entry into force 30.06.2021]

(4) Based on the national risk assessment, the minister in charge of the policy sector 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 in charge of the policy sector and related fields;
5) pursue national cooperation in AML/CFT and in countering proliferation.

(2) The AML/CFT Committee consists of the minister in charge of the policy sector, 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 and Resolution Authority, and representatives of other relevant bodies and governmental authorities.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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 in charge of the policy sector.

(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 create a document showing assessment of the risks, 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.

(1^1) As a result of assessment of the risks, the crypto-asset service provider defines the money laundering and terrorist financing risk in relation to crypto-asset transfers to or from a self-hosted address.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(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 an obliged entity may, at the request of the obliged entity, except for an obliged entity subject to supervision by the Financial Supervision and Resolution 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 of the field characteristic of the obliged entity 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.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(6) 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.
[RT I, 10.07.2020, 1 – entry into force 01.01.2021]

Subchapter 2
Risk Management System of Obliged Entity

§ 14. Rules of procedure and internal control rules

(1) The obliged entity 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 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;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
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.

(1[1]) Credit institutions and financial institutions must, before applying special rules provided by § 31 of this Act concerning due diligence measures, establish rules of procedure that ensure secure identification of persons and verification of data, and that effectively alleviate and manage risks related to application of due diligence measures without being present in the same location as the person.
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

(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 whether 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) When performing the obligation provided by clause 2 of subsection 1 and by subsection 1[1] of this section, the credit institution as well as the financial has regard to relevant guidelines of the competent supervisory authority as well as of the European Banking Authority and of the data protection supervisory authority.
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

(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 manager 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 activities 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 entity 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 in charge of the policy sector 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 Banking Authority 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.
[RT I, 14.04.2021, 1 – entry into force 30.06.2021]

(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 a right to issue a compliance notice 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 paragraph 7 of Article 45 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 is shared, unless the Financial Intelligence Unit has instructed otherwise.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(6) An e-money institution, payment service provider or crypto-asset service provider who operates in Estonia in a form other than a branch and whose headquarters are in another Member State of the European Union appoints, on the basis of an order made by the competent supervisory authority and in accordance with regulatory technical standards established by the European Commission on the basis of paragraph 9 of Article 45 of Directive (EU) 2015/849 of the European Parliament and of the Council, a central contact point in Estonia whose function is to ensure, on behalf of the e-money institution, payment service provider or crypto-asset 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.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(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

(1) Obliged entities may cooperate with one another for AML/CFT purposes, thereby communicating information available to them and replying to queries within a reasonable time, following the duties, obligations and restrictions arising from legislation.

(2) Obliged entities may exchange information that one of them needs and the other has obtained for the application of a due diligence measure arising from clause 1, 3 or 5 of subsection 1 of § 20 of this Act, following the restrictions established in this Act and the principle of good faith, regardless of any banking, business, official, professional or other confidentiality obligation or restriction on sharing information provided for in any other Act.

(3) Subsection 2 of this section does not apply where the obliged entity assesses a customer’s legal position, defends or represents the customer in court, intra-authority appeal or other such proceedings, including consults a customer regarding the institution or avoidance of proceedings, regardless of whether the information has been received before, during or after the proceedings.

(4) Information obtained on the basis of subsection 2 of this section may be used solely for the performance of the duties and obligations arising from this Act, taking into account all of the requirements provided for in this Act, including the data collection, retention and protection rules. The scope and manner of communication or exchange of information between obligated entities is agreed on at least in a form reproducible in writing.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(5) In implementing subsections 1 and 2 of this section, the obliged entities may exchange, among other things, information on sanctions arising from the legislation specified in § 9 of the International Sanctions Act and other agreements binding upon the obliged entity. It is permitted to use the obtained information solely for the performance of duties established by legislation, taking into account all of the requirements provided for in this Act, including rules on collection, retention and protection of data. The scope and manner of communication of information between obliged entities is agreed on in a form that is at least reproducible in writing.
[RT I, 14.04.2021, 1 – entry into force 24.04.2021]

§ 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 or the manager of a branch of a credit institution, financial institution or obliged entity specified in subsection 1 of § 70 of this Act appoints a person to act as a contact person of the Financial Intelligence Unit (hereinafter *compliance officer*). The compliance officer reports directly to the management board of the obliged entity or to the manager of the branch and has the competence, means and access to relevant information across all of the structural units of the obliged entity.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(3) A compliance officer may also be appointed by an obliged entity not specified in subsection 2 of this section.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(5) Only a person who works permanently in Estonia and has the education, professional suitability, 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(6) The Financial Intelligence Unit has a 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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;
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]
3) periodic submission of written statements on compliance with the requirements arising from this Act to the management board or branch manager of the obliged entity;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
4) performance of other duties and obligations related to compliance with the requirements of this Act.

(8) A compliance officer has a right to:
1) make proposals to the management board or branch manager of the obligated entity 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;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
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 manager 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

Subchapter 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 the value of the transaction is at least 15,000 euros or an equivalent sum in another currency, regardless of whether the financial obligation is performed in the transaction as a single payment or as several related payments over a period of up to one year, unless otherwise provided by law;
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]
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 at least 10,000 euros or of an equivalent sum in another currency is made to or by the trader in cash, regardless of whether the monetary obligation is performed as a single payment or as several related payments over a period of up to one year.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(2^1) A foundation, non-profit association or an entity to which the provisions of the Non-profit Associations Act apply applies due diligence measures at least every time when it is paid or it pays in cash an amount of over 5,000 euros as a single payment or as several related payments over a period of up to one year.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2^2) A person who mediates real property usage transactions applies due diligence measures at least every time when the value of the usage fee agreed on in the transaction amounts to no less than 10,000 euros a month.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2^3) A dealer of works of art and a person who mediates works of art or stores them in a customs free zone applies due diligence measures at least every time they are paid or they pay a sum with a value of at least 10,000 euros as a single payment or as several related payments over a period of one year.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2^4) In addition to what is provided for in subsection 1 of this section, a provider of trust or company services applies due diligence measures on each occasion when it provides the service mentioned in clause 1 of § 8 of this Act;

[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(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 2,000 euros or an equivalent sum in another currency, regardless of whether the monetary obligation is performed as a single payment or as several related payments over a period of up to one month.

(4) [Repealed – RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(5) The obliged entity applies the due diligence measures provided in clauses 1–5 of subsection1 of § 20 of this Act before the establishment of a business relationship or the making of a transaction outside a business relationship, unless otherwise provided for in this Act.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(5^1) The auditor auditing an annual report or carrying out an inspection applies the due diligence measures specified in clause 3 of subsection 1 of § 20 of this Act during the audit or inspection, thereby examining the information gathered by the management board of the customer in accordance with subsection 2 of § 76.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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 related payments, as soon as the sum is exceeded.

(7) The provisions of this Chapter regarding cash are also applicable to the performance of monetary 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 representative of a customer or 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 operation 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 their 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, whether they act for or on behalf of another and, in the case of a legal person, also the experience of the customer or person participating in the occasional transaction.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2^1) Where the obliged entity establishes a business relationship with a customer whose information on beneficial owners must, in accordance with the statutes of a Member State of the European Union, be submitted to the state or be registered there, the obliged entity must obtain a relevant registration certificate or registry extract upon application of clause 3 of subsection 1 of this section.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2^2) [Repealed – RT I, 02.06.2021, 1 – entry into force 12.06.2021]

(2^3) [Repealed – RT I, 02.06.2021, 1 – entry into force 12.06.2021]

(2^4) Where, in the course of acting on clause 3 of subsection 1 of this section, the obliged entity learns any particulars that differ from those published in accordance with § 78 of this Act, the entity – except in a situation mentioned in subsection 1 of § 49 – notifies this within a reasonable time to the Registrar of the Commercial Register. The information or documents that show the difference are attched to the notification made under this subsection.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(2^5) The obligation specified in subsection $2^4$of this section does not apply to an auditor conducting an audit or inspection of a customer's annual accounts, provided the customer eliminates the discrepancy by the time the auditor's opinion or summary of the inspection is signed.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(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) The person participating in a transaction made in economic or professional activities, the person participating in a professional operation or the person using a professional service or the customer submits, at the request of the obliged entity, documents required for the application of the due diligence measures and provides relevant information. The person participating in a transaction made in economic or professional activities, the person participating in an official operation or the person using an official service or the 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.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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, operation 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 entity 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 an official operation;
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) the person's name;
2) their personal identification code or, where the person does not possess one, their date of birth and the place of residence or location;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
3) information concerning recognition 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 that right, its date of issue, and the name of the issuer;
4) particulars of the person's means of telecommunication.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(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.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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.

(5) The two sources requirement specified in subsection 4 of this section does not need to be followed with regard to a customer who has limited active legal capacity and in the name of whom a business relationship is established or a transaction is made by their representative.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

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

(1) The obliged entity 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 person's name or business name;
2) the person's registry code or registration number and the date of registration;
3) the names of the person's sole director, of members of the person's management board or other body replacing the management board, and the scope of their authority to represent the legal person;
4) particulars of the person's means of telecommunication.

(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 equivalent 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 equivalent 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, professional or official 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, professional or official 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, professional or official 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.

Subchapter 2

Variations of Application of Due Diligence Measures

§ 24. Reliance on data gathered by another 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 subsection 1 of § 20 of this Act, rely on data and documents gathered by another person, where all the following criteria are met:
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
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 without delay 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 regulatory enforcement 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 subsection 1 of this section, the obliged entity may also outsource an activity related to the implementation of clauses 1–5 of subsection 1 of § 20 of this Act to:
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
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 by this Act or participates in applying due diligence measures and who is under a contractual obligation to preserve data gathered in the course of application of such measures and to make these available to the supervisory authority.
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

(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 a 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 without delay.

(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 entity 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, provider of virtual currency service and Eesti Pank

[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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.

(1^1) Credit institutions and financial institutions must apply due diligence measures when effecting a money transfer made as an occasional transaction outside a business relationship if the value of the transaction exceeds 1,000 euros or an equivalent sum in another currency regardless of whether the monetary obligation is performed in the transaction as a single payment or as several related payments over a period of up to one month.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(1^2) The currency exchange service may be provided without identifying the person participating in the transaction of the value of the amount exchanged in cash in a one-off transaction or in linked transactions does not exceed 1,000 euros.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(1^3) Providers of virtual currency services and crypto-asset service providers are not allowed to provide services outside a business relationship.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(2) Credit institutions, financial institutions and providers of virtual currency services are not allowed to conclude a contract or make a decision to open an anonymous account, savings book, virtual currency wallet, crypto-assets account or safe-deposit box. Transactions violating this prohibition are void.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(2^1) A payment service provider providing a payee with a payment service does not accept a payment made with an anonymous prepaid card whereby all of the following requirements have not been met:
1) the prepaid card is not reloadable and the maximum amount stored thereon electronically does not exceed 150 euros;
2) the prepaid card is used solely for purchasing goods or services;
3) the prepaid card cannot be financed using anonymous e-money;
4) the issuer of the prepaid card sufficiently monitors transactions or the business relationship in order to identify unusual or suspicious transactions;
5) the payment does not exceed 50 euros.
[RT I, 10.07.2020, 1 – entry into force 10.01.2021]

(2^2) When ascertaining a person's identity, a provider of virtual currency services and a crypto-asset service provider must collect, as contact particulars, at least the person's telephone number and e-mail address.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(2^3) When providing the service of exchange or transfer of virtual currency, a provider of virtual currency service is obligated to apply at least the due diligence measures provided by subsections 2^4, $2^5$and $2^7$of this section.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(2^4) When performing a transaction of exchange or transfer of virtual currency, the transaction initiator's provider of virtual currency service ascertains the identity of each customer according to the provisions of §§ 21 and 22 of this Act, and, with respect to the initiator, collects at least the following particulars:
1) for a natural person – the person's name, unique identifier of the transaction, identifier of the payment account or virtual currency wallet, the title and number of the identity document and personal identification code or date and place of birth and residential address;
2) for a legal person – the person's name, unique identifier of the transaction, identifier of the payment account or virtual currency wallet, the person's registry code or, where it does not have one, the relevant identifier in the country of its seat (a combination of numbers or letters equivalent to a registration number), and the address of the seat.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(2^5) When effecting a transaction of virtual currency exchange or transfer, a provider of virtual currency service collects, with respect to the virtual currency or to the recipient of the transfer, the particulars of the transaction's unique identifier and, where the particulars of the identifier of a payment account or virtual currency wallet are used to perform the transaction, also those particulars.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(2^6) For the purposes of this section, 'unique identifier' of a transaction means a combination of letters, numbers or symbols which is assigned by the virtual currency service provider in accordance with the protocol of the system used to perform the transaction and which allows the transaction to be followed from its initiator to the recipient of the transfer.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(2^7) The transaction initiator's virtual currency service provider transmits the particulars mentioned in subsections $2^4$and $2^5$of this section without delay and securely to the recipient's virtual currency service provider. Transmission of the particulars may be arranged together with transmission of the set of payment instructions to the recipient's virtual currency service provider or to the recipient's credit or financial institution.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(2^8) Where the recipient's virtual currency wallet does not have a provider of virtual currency service or the recipient's provider is unable to receive or process the data, the obligation described in subsection $2^7$of this section is deemed to be fulfilled if the transaction initiator's virtual currency service provider ensures – by using an appropriate technical solution – the monitoring of the transactions in real time and risk analysis in respect of each transaction, and if that provider preserves the particulars mentioned in subsections $2^4$and $2^5$of this section by a method that allows them to be produced without delay when a corresponding request is made by a regulatory enforcement, supervisory or oversight or investigative authority.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(3) Eesti Pank applies the due diligence measures specified in clauses 1–5 of subsection 1 of § 20 of this Act.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(4) Eesti Pank applies the due diligence measures specified in clauses 1–5 of subsection 1 of § 20 of this Act 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.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 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 without delay 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 2 of § 7 of the Commercial Register Act, 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 1–5 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.
[RT I, 05.05.2022, 1 − entry into force 01.02.2023]

§ 28. Due diligence measures applicable to trusts and legal arrangements

[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
In addition to the due diligence measures specified in subsection 1 of § 21 of this Act, the credit institution or financial institution gathers enough information on the beneficiaries of a trust or legal arrangement, which has been determined based on certain characteristics or type, in order to be certain that it is able to definitely identify the beneficiary at the time of making a payment or once the beneficiary exercises their rights.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 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 1–5 of subsection 1 of § 20 of this Act.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2) The persons specified in subsection 3 of § 2 of this Act apply the due diligence measures specified in clauses 1–5 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.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 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 agent, 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 event specified in subsection 2 of this section, the application of due diligence measures must be completed within a reasonable time after the first contact and before making binding operations.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 31. Special rules for due diligence measures applied by credit institutions, financial institutions and notaries when performing remote identification of persons

[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

(1) A credit institution and a financial institution are required to identify persons and verify data based on rules of procedure that meet the requirements provided by subsection $1^1$of § 14 of this Act and that ensure secure identification of persons and verification of data, and are required to employ a scheme or service mentioned in subsection 3 of this section or a means or service that meets the requirements of subsection $3^1$where due diligence measures are not applied in a situation of presence in the same location as the person and where:
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]
1) the customer's place of residence or seat is in a country outside the European Economic Area, or
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]
2) the total amount of outgoing payments related to the transaction or service contract per calendar month exceeds 15,000 euros in the case of a customer who is a natural person or 25,000 euros in the case of a customer who is a legal person.
[RT I, 10.07.2020, 1 – entry into force 10.09.2020]

(1^1) When performing the obligation provided by subsection 1 of this section, the credit institution and the financial institution must employ a schme or service provided for by subsection 3 where the residence or seat of the customer or of the person who carries out the occasional transaction is in a high-risk third country or in a jurisdiction that falls under the provision of clause 4 of subsection 4 of § 37 of this Act.
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

(2) [Repealed – RT I, 10.07.2020, 1 – entry into force 10.09.2020]

(3) Where due diligence measures are not applied in a situation of presence in the same location with the person, the following are allowed to be used for identifying the person and verifying data:
1) an electronic identification scheme that has been notified in accordance with Article 9 of Regulation (EU) 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, p. 73) and that corresponds to the assurance level provided for by subparagraph (b) or (c) of paragraph 2 of Article 8 of that Regulation;
2) a qualified trust service that meets the requirements provided by Regulation (EU) 910/2014 of the European Parliament and of the Council.
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

(3[1]) Where due diligence measures are not applied in a situation of presence in the same location with the person, and it is not possible to employ a scheme or service mentioned in subsection 3 of this section, the means or service used to identify the person and verify data must ensure:
1) that the data and documents gathered in the course of applying due diligence measures are correct and up to date;
2) secure gathering and storage of images, video, audio and data in understandable form and with sufficient quality, such that unambiguous identifiability of the person is ensured;
3) in a situation where the connection is unexpectedly interrupted or on manifestation of other technical defects, the failure of identification.
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

(4) Where due diligence measures are not applied in a situation of presence in the same location with the person and an e-resident's digital identity document is used to identify the person and verify data, another document mentioned in subsection 3 of § 21 of this Act must be used simultaneously.
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

(5) To identify the person and verify data, the credit institution and the financial institution may use personal identification data recorded in the database of identity documents.
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

(6) When performing the obligations provided by this section, the credit instiution and the financial institution have regard to what has been provided in the relevant guidelines and instructions of the competent supervisory authority and of the European Banking Authority.
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

(6[1]) The procedure provided for in a regulation established on the basis of subsection 1 of § 31 of the Notaries Act is applied where the identity of a person is established and information is verified using information technology means in the official activities of a notary.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(7) [Repealed – RT I, 21.06.2024, 3 – entry into force 01.07.2024]

Subchapter 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 operation is of a lower risk and the credit institution and financial institution attribute to the transaction, operation 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, operations 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 at 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) a limit has been set to the total value of incoming and outgoing payments in transactions.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 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 Banking Authority regarding risk factors.
[RT I, 14.04.2021, 1 – entry into force 30.06.2021]

(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 monetary limits or transparency-enhancing measures;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
6) basic payment services relating to a liability account.

Subchapter 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 a transaction made in economic or professional activities, the person participating in an official operation, the person using an official service or the customer is a politically exposed person, except in the event specified in subsection 5 of § 38 of this Act;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
3) the person participating in a transaction made in economic or professional activities, the person participating in an official operation, the person using an official 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 person participating in the transaction or the person using an official 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 has been entered in the EU list of non-cooperative jurisdictions for tax purposes;
[RT I, 26.03.2021, 1 – entry into force 01.01.2022]
5) the customer or person participating in the transaction or the transaction itself has a connection to a country or jurisdiction which, according to reliable sources, is characterised by a significant level of corruption or other criminal activity – or against which sanctions, an embargo or other similar measures have been imposed – and a scheme or service mentioned in subsection 3 of § 31 of this Act is not used when applying the special rules provided by § 31 for due diligence measures;
6) transactions of transfer of crypto-assets are directed to or emanate from a self-hosted address.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(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;

7) the customer is a third country national who applies for residence rights or citizenship in Estonia in exchange of capital transfers, purchase of property or government bonds, or investment in corporate entities in Estonia.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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;
6) a transaction related to oil, arms, precious metals, precious metal products or tobacco products;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
7) a transaction related to cultural artefacts or other items of archaeological, historical, cultural and religious importance, or of rare scientific value;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
8) a transaction related to ivory or protected species.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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 as well as a financial institution takes into account, in addition to subsections 2–4 of this section, relevant guidelines of the European Banking Authority regarding risk factors.
[RT I, 14.04.2021, 1 – entry into force 30.06.2021]

§ 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) the gathering of 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) the gathering of 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) the gathering of 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
7) the gathering of additional information regarding the origin and destination of the crypto-asset transferred.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(3) When applying 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 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 Banking Authority upon selection of due diligence measures.

[RT I, 14.04.2021, 1 – entry into force 30.06.2021]

(4[1]) When selecting and applying additional due dilience measures, the crypto-asset service provider has regard to relevant guidelines of the European Banking Authority.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(5) In addition to the measures provided for in this section, the measures provided for in § 41 of this Act also apply to a politically exposed person, their family member or a person known to be their close associate. Where there is a factor that refers to a lower risk specified in clause 1 of subsection 3 of § 34 of this Act regarding the aforementioned person, the application of the aforementioned measures is required only where there is a factor referring to a higher risk.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 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 an official operation, via a person using an official 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 or transaction patterns that are additionally verified;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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. Duties and obligations of correspondent institution

[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(1) In the case of a cross-border correspondent relationship with a respondent institution of a third country or a respondent institution whereby the risk of money laundering or terrorist financing is higher, the credit institution or the 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:
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
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 customers who have direct access to accounts of the correspondent institution, applies due diligence measures to them on a continual basis and, where this is requested, is able to state relevant particulars of the due diligence measures applied to the customer.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(1[1]) A crypto-asset service provider ascertains whether the crypto-asset service provider that appears as the respondent institution holds the authorisation or – where the crypto-asset provider that appears as the customer is established in a third country – whether they hold the registration.

[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(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 obtain all data and documents without delay 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.

(5) When establishing a correspondence relationship and providing correspondence services, the crypto-asset service provider has regard to relevant guidelines of the European Banking Authority.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

§ 41. Transactions with politically exposed person

(1) In a situation where the person participating in a transaction made in economic or professional activities, the person participating in an official operation, the person using an official service, the 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 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) 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) [Repealed – RT I, 10.07.2020, 1 – entry into force 20.07.2020]

Subchapter 5
Consequences of Failure to Apply Due Diligence Measures

§ 42. Prohibition on making transactions and establishing business relationships

[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(1) The obliged entity is not allowed to establish a business relationship or enable the making of an occasional transaction or the making of a transaction in a business relationship where at least one of the following circumstances occurs:

1) the obliged entity is unable to apply the due diligence measures required under this Act;
2) the obliged entity suspects money laundering or terrorist financing.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2) The obliged entity is prohibited to establish a business relationship or make a transaction with a person of whose capital consists of bearer shares or other bearer securities to the extent of more than 10 per cent.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(3) A payment service provider, a provider of virtual currency service and a crypto-asset service provider are prohibited from carrying out a customer's payment instruction or making funds, virtual currency or crypto-assets available if they are unable to fulfil the obligations provided by § 25 of this Act. A provider of virtual currency service must, in accordance with internal procedures established following risk analysis, lay down rules that regulate when virtual currency amounts are to be transferred back to the transaction initiator and when they are not to be made available to the transaction recipient. When applying subsection 2^8 of § 25 of this Act, a provider of virtual currency service must, when it recognises the presence of increased risk and considers whether to notify the Financial Intelligence Unit of a suspicious transaction following the rules provided by § 49, take into account the completeness and sufficiency of the particulars of the transaction initiator and the recipient.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(7) Subsections 1–5 of this section do not apply to an auditor that provides a customer with a certainty-giving or related auditor service or accounting revision service and that has reported the occurrence of the circumstances specified in subsection 1 or 2 to the Financial Intelligence Unit in accordance with the procedure provided for in § 49 of this Act.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 43. Right to postpone transactions and terminate business relationships

[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(1) The obliged entity has a right to postpone the making of a transaction until the person participating in the transaction or official operation, a person using an official service or a customer has submitted the documents and information required for the application of due diligence measures, including for certifying the origin of the subject-matter of the transaction or for monitoring the business relationship.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2) The obliged entity has a 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) [Repealed – RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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 without delay after making the transaction or deciding to continue the business relationship in accordance with the procedure provided for in § 49 of this Act.

[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 44. Restrictions on transfer of customer's property

(1) Upon implementation of the provisions of this Subchapter, the obliged entity may transfer the customers 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 establish the restriction specified in § 57 of this Act.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) Upon opening an account to a company established in the manner provided for in subsection2 of §27 of this Act, subsection 1 of this section is applied, unless the Financial Intelligence Unit has established a different procedure by a compliance notice issued under § 55 of this Act.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 45. Variations upon provision of legal service

The provisions of this Subchapter do not apply to a notary, enforcement agent, bankruptcy trustee, 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 customers legal status or in performing duties as the customers defence counsel or representative in court proceedings or in connection therewith, including in connection with giving advance on the initiation or avoidance of proceedings.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

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 the person participating in the transaction or official operation, the person using an official service or the customer where the waiver is related to the application of due diligence measures by the obliged entity;
2^1) information on all of the operations made for the purpose of establishing the identity of a person participating in a transaction or official operation, a person using an official service or a customer;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
3) information, where in applying § 31 of this Act it is not possible to apply the due diligence measures provided by subsection 1 of § 20;
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]
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 the representative of a civil law partnership, community or another legal arrangement or with a trust 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.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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 cases of transfers of funds or of crypto-assets, the particulars whose retention is mandatory under Regulation (EU) No 2023/1113 of the European Parliament and of the Council;
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]
8) in the case of another transaction, the transaction amount, the currency and the account number.

§ 47. Preservation of data

(1) For the purpose of identification of persons and verification of submitted information, the obliged entity must retain the originals or copies of the documents specified in subsection 2^1 of § 20 and §§ 21, 22 and 46 of this Act, information registered in accordance with § 46 and the documents serving as the basis for the establishment of a business relationship for no less than five years after the termination of the business relationship.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(1^1) The obliged entity does not have to retain the originals or copies of the documents serving as a basis for the identification of persons and verification of submitted information where:
1) the person was identified using e-identification and trust services for e-transactions, or
2) the document is available to the obliged entity in an electronic database of the state throughout the period specified in subsection 1 of this section.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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 or occasional transactions as well as data on suspicious or unusual transactions or circumstances which were not reported to the Financial Intelligence Unit.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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, 2 and 3 of this section in a manner that allows for exhaustively and without delay 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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.

(5^1) A provider of virtual currency service must preserve any documents, copies of documents and particulars related to fulfilment of the obligations provided by subsections 22–2^5, 2^7 and 2^8 of § 25 of this Act for five years following termination of the business relationship with the customer.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(6) When applying § 31 of this Act, the obliged entity retains the data of the document prescribed for digital identification of the person, information on the making of an electronic query to the identity documents database, and the data – including the time stamp – of the procedure of identifying the person and verifying their identity for five years following termination of the business relationship.
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

(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 compliance notice issued by 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, which is considered a matter of public interest for the purposes of Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 04.05.2016, pp 1–88), and such data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2^1) The following rights of the data subject may be limited with regard to personal data processed by the obliged entity based on § 16 of this Act:
1) to demand the restriction of the processing of their personal data;
2) to demand the portability of their personal data;
3) to object to the processing of their personal data.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2^2) On the basis of subsection 2^1 of this section the rights of the data subject may be restricted where the non-restriction may harm the ability of the processor or another obliged entity to comply with the requirements of this Act, including to apply due diligence measures.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(3) The obliged entity presents to new customers information concerning the processing of personal data before establishing a business relationship or making an occasional transaction with them. Such information includes general information on the duties and obligations of the obliged entity which apply for AML/CFT purposes when the entity processes personal data.

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, an official operation or provision of an official 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 without delay, but not later than within two working days after identifying the activity or facts or after getting the suspicion.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) Subsection 1 of this section also applies where a business relationship is not established, a transaction or operation is not made or a service is not provided, and the application thereof is considered also in the event of the circumstances specified in §§ 42 and 43 of this Act.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(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 monetary obligation of over 32,000 euros or an equivalent sum in another currency is performed in cash, regardless of whether the transaction is made as a single payment or as several related payments over a period of up to one year. The credit institution notifies the Financial Intelligence Unit without delay, 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(3^1) The auditor who, in the course of whose professional activities, learns of a transaction which another obliged entity should have reported to the Financial Intelligence Unit under subsection 3 of this section, reports it to the Financial Intelligence Unit not later than within two working days after receiving the information.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(4) The obliged entity submits to the Financial Intelligence Unit without delay all the information available to the obliged entity, which the Financial Intelligence Unit requested in its enquiry.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(5) The duty to report, which arises from subsections 1–4 of this section, does not apply to a notary, enforcement agent, 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 official operation 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 official operation will be performed out or the official service will be provided and a report will be submitted to the Financial Intelligence Unit thereafter.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 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 has been established.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2) A report is submitted via the online form of the Financial Intelligence Unit or via the X-road service.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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 report submitted to the Financial Intelligence Unit and the guidelines for the submission of a report are established by a regulation of the minister in charge of the policy sector.

§ 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 compliance notice issued by the Financial Intelligence Unit under §§ 57 and 58 of this Act or about the commencement of criminal proceedings. After the compliance notice issued 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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 agent, 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 agents, 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 official secrets and protecting personal data.

(4) Where a notary, enforcement agent, 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 an official operation or in the provision of an official 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 compliance notice issued by 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(4) Taking into account its size and nature of activities, the obliged entity establishes an appropriate system of measures ensuring that the employees and representatives of the obliged entity who report of a suspicion of money laundering or terrorist financing or of a violation of this Act within the obliged entity are able to do so anonymously and 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.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 52[1]. Protection of originator of report

(1) The Financial Intelligence Unit and the Financial Supervision and Resolution Authority ensure the confidentiality of the fact of reporting of a violation of this Act as well as of a factor the reporting specified in § 49 of this Act and this fact may be disclosed only with the written consent of the natural person who filed the report.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) The fact of reporting may be disclosed to the prosecutor’s office and the investigation body where there is a suspicion that the person who filed the report has violated the reporting obligation or committed a criminal offence.

(3) Where the natural person who filed a report is involved in offence proceedings as a witness, the provisions of the offence proceedings apply without compromising the confidentiality of the fact of reporting.

(4) The employer is not allowed to treat an employee unequally because of a report specified in subsection 1 of this section.

(5) The court or the labour dispute committee applies a shared burden of proof for the purpose of protection of the natural person who filed the report. The claimant or petitioner submits in the claim or petition the facts based on which it can be concluded that they have been treated unequally. Where the person against who the claim or petition has been filed does not prove otherwise, it is presumed that the originator of the report was treated unequally due to reporting. An agreement deviating from this subsection is void.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

Chapter 6
Financial Intelligence Unit

[RT I, 21.11.2020, 1 - entry into force 01.01.2021]

§ 53. Financial Intelligence Unit

[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(1) The Financial Intelligence Unit is a governmental authority in the area of government of the Ministry of Finance, which is autonomously engaged in regulatory enforcement and autonomously exercises the enforcement powers of the state on the grounds and to the extent provided for in this Act. The Financial Intelligence Unit independently performs its tasks under this Act and independently makes decisions concerning the actions provided for in this Act.

(2) The Government of the Republic appoints the head of the Financial Intelligence Unit to office on a proposal of the Minister of Finance for a period of five years, taking into account the procedure established on the basis of subsection 2 of § 10 of the Civil Service Act.

(3) The costs of the Financial Intelligence Unit are covered from the state budget. The Financial Intelligence Unit has its own budget that is approved and revised by the Minister of Finance on a proposal of the head of the Financial Intelligence Unit in accordance with the statutory procedure. The Minister of Finance oversees adherence to the budget of the Financial Intelligence Unit.

(4) The roster of service and employment positions and the roster of staff of the Financial Intelligence Unit constitute 'information for internal use' for the purposes of the Public Information Act.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 54. Duties of Financial Intelligence Unit

(1) The duties of the Financial Intelligence Unit:
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]
1) prevention of money laundering and terrorist financing and the receiving, gathering, obtaining of the disclosure, registration, processing, analysis and transmission of information referring to money laundering and terrorist financing;
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]
2) strategic analysis that covers the risks, threats, trends, patterns and ways of operation of money laundering and terrorist financing;
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]
3) application of the enforcement powers of the state on the grounds and within the scope provided by a statute;
[RT I, 10.07.2020, 1 – entry into force 01.01.2021]
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 are important for countering, identifying or pre-litigation investigation of money laundering, related criminal offences and terrorist financing.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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 forwards materials to the competent authorities without delay upon identification of elements of a criminal offence. The competent authority notifies the Financial Intelligence Unit without delay of having attached, having decided not to attach or of having released an attachment of property in accordance with the procedure established in the Code of Criminal Procedure.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 54[1]. Reports submitted to Financial Intelligence Unit

[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(1) Credit and financial institutions and persons subject to supervision exercised by the Financial Intelligence Unit under subsection 1 of § 64 of this Act submit to the Financial Intelligence Unit reports containing information necessary for the performance of the statutory functions.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) The collection and submission of the information specified in subsection 1 of this Act may also be organised with the help of governmental authorities, state authorities and public legal persons. The principle of the single submission of information must be adhered to regarding the obliged entity.

(3) The requirements for the content and originator of reports submitted to the Financial Intelligence Unit and the procedure for submission are established by a regulation of the minister in charge of the policy sector.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 55. Administrative decisions of Financial Intelligence Unit

[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(1) The Financial Intelligence Unit issues compliance notices and other administrative decisions in order to perform the duties arising from law.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) A compliance notice issued under § 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 compliance notice 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 based on which the notice 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 compliance notice has a right to examine the document setting out the facts. The Financial Intelligence Unit has a right to refuse to grant access to the document where:
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]
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 or employee authorised by the Head. Where a decision is signed by an authorised official or employee, the number and date of the document granting the right to sign and the place where it is possible to acquaint oneself with that document are stated next to the signature.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(5) A claim against an administrative decision or step of the Financial Intelligence Unit is filed with the administrative court. Upon contesting a compliance notice mentioned in subsection 2 of this section, the Financial Intelligence Unit submits to the administrative court a separate document setting out the facts, which states the reasons for issuing the notice, establishing relevant restrictions concerning the document.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 56. Guidelines of Financial Intelligence Unit

[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(1) The Financial Intelligence Unit has a right to issue advisory guidelines to explain AML/CFT legislation.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) The Financial Intelligence Unit issues guidelines regarding the characteristics of suspicious transactions.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(4) The guidelines of the Financial Intelligence Unit are published on its website.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 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 compliance notice 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, official operation or official 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 compliance notice. 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(3) By means of a compliance notice, 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:
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]
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;
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]
2) there is suspicion that the property is used for terrorist financing.

(4) In enforcement or bankruptcy proceedings it is prohibited to transfer property on which a restriction has been imposed by the Financial Intelligence Unit or which has been attached during the validity of the restriction in accordance with the rules provided for in the Code of Criminal Procedure.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(5) Where property has been attached in accordance with the Code of Criminal Procedure, the Financial Intelligence Unit is required to without delay lift the restrictions on the disposal of the property after a court order on the attachment of the property has entered into effect.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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 a 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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 without delay, without any additional steps taken by the Financial Intelligence Unit.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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 terminate the restrictions of use of the property without delay.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 58. Requesting information

(1) To perform the duties arising from law, the Financial Intelligence Unit has a right to receive information from the competent supervisory authorities, other state authorities and local authority agencies and, based on a compliance notice, from obliged entities and third parties by the deadline set by the Financial Intelligence Unit.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(1[1]) To perform the functions arising from this Act, the Financial Intelligence Unit has a right to receive the information specified in subsections 1[1]–1[5] of § 81 of this Act via the electronic attachment system mentioned in § 63[1] of the Code of Enforcement Procedure.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) The addressee of a compliance notice is required to comply with the notice and to submit the requested information, including any information subject to banking or business secrecy, within the time limit set in the notice. The information is submitted in writing or in a form reproducible in writing.

(3) In order to prevent money laundering and terrorist financing, the Financial Intelligence Unit has a right to obtain, in accordance the procedure provided by legislation, relevant data, including data collected by covert operations and covert cooperation, from any agency vested with the authority to conduct covert operations by the deadline set by the Financial Intelligence Unit. Where the Financial Intelligence Unit wishes to forward information collected by way of covert operations and covert cooperation to other authorities, the Financial Intelligence Unit must obtain written consent from the covert operations agency that provided the information.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 59. Interbase cross-usage of data

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

§ 59[1]. Database of Financial Intelligence Unit

[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(1) The database of the Financial Intelligence Unit is a database that is part of the information system of the state, which processes data related to the operations and proceedings arising from the functions of the Financial Intelligence Unit.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) The Financial Intelligence Unit is the controller of the database.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(3) The statutes of the database are established by a regulation of the minister in charge of the policy sector.
[RT I, 10.07.2020, 1 – entry into force 01.01.2021]

§ 60. Restrictions on the use of data

(1) Only an official or an employee of the Financial Intelligence Unit has access to and a 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 officials and employees of the Financial Intelligence Unit as well as other persons who have access to information contained in the database are required, for an unspecified period of time, to keep confidential any information known to them about money laundering or terrorist financing.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(2) For prevention and identification as well as pre-trial investigation of money laundering or terrorist financing or related criminal offences, the Financial Intelligence Unit must transmit material information, including information containing tax and banking secrets, to the Prosecutor's Office, the investigative authority and the court.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(3) Data registered in the Financial Intelligence Unit are transmitted strictly, in connection with criminal proceedings, to the authority that conducts pre-trial proceedings, to the prosecutor or to the court on a written request of the authority, prosecutor or court, or of the Financial Intelligence Unit's own motion where transmission is required for the prevention, identification and investigation of money laundering or terrorist financing and of related criminal offences as well as, in administrative court proceedings, to the administrative court that deals with a request of the Financial Intelligence Unit or an appeal or objection filed against an operation or administrative decision of the Unit.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(4) The Financial Intelligence Unit may notify the competent supervisory authority of a breach, by an obliged entity, of the requirements of this Act or, on a relevant request, transmit data, analyses or assessments registered

in the Unit to the authority insofar as this does not violate any restrictions established in the framework of law or treaty 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(5) The Financial Intelligence Unit may transmit the information mentioned in subsection 4 of this section to the Tax and Customs Board to be used in proceedings related to gambling activity licences.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(5^1) The Financial Intelligence Unit may transmit the information mentioned in subsection 4 of this section to the Police and Border Guard Board for deciding to issue, suspend or revoke an e-resident's electronic identity card, or to issue or extend, or refuse to issue or extend, or revoke, the residence permit to pursue entrepreneurial activities as a large investor.
[RT I 10.02.2023, 3 – entry into force 20.02.2023]

(5^2) For assessing the reliability of a foreign investment, the Financial Intelligence Unit may transmit the information mentioned in subsection 4 of this section to the Consumer Protection and Technical Regulatory Authority and to the Foreign Investment Committee.
[RT I 10.02.2023, 3 – entry into force 01.09.2023]

(5^3) For purposes of proceedings concerning the authorisation provided for by Regulation (EU) 2023/1113 of the European Parliament and of the Council, the Financial Intelligence Unit may transmit the information mentioned in subsection 4 of this section to Estonian Financial Supervision and Resolution Authority.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(6) With the permission of the Head of the Financial Intelligence Unit, persons whose involvement is required for the performance of the Unit's duties may be granted temporary access to data to the extent that is required and sufficient for them to perform their duties. The authority and powers of the person who has been granted the permission are governed by the provisions of subsections 1–5^2 of this section and by § 61 of this Act as applicable to the Unit's officials or employees.
[RT I, 10.02.2023, 3 – entry into force 01.09.2023]

(7) In an individual case, the Financial Intelligence Unit may transmit, to the compliance officer of the obliged entity, the data registered in the Financial Intelligence Unit to the extent that this is required and sufficient for the purpose of taking joint AML/CFT measures or measures for the prevention of related criminal offences.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(8) The Financial Intelligence Unit may establish restrictions on the use of transmitted data which the user of the data is bound to follow.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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 so handed over after the passing of 30 years, following which the documents and records are deleted from the Unit's database. Until they are handed over, the documents and records are preserved at the Unit.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(10) [Repealed – RT I, 10.07.2020, 1 – entry into force 01.01.2021]

§ 61. Requirements for officials and employees of the Financial Intelligence Unit

[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(1) Only a person with impeccable reputation, the required experience, abilities, education and the requisite high moral qualities may be appointed as an official or hired as an employee of the Financial Intelligence Unit.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(2) Officials and employees of the Financial Intelligence Unit are required to maintain as confidential any information they become privy to in the course of their official or employment duties, including information subject to banking, business, office-related, professional or other secrecy or information subject to disclosure restrictions, also after the performance of their official or employment duties in relation to the processing or use of such information or the termination of their service or employment relationship.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 61[1]. Security vetting

(1) In order to assess whether a person is fit to be appointed an official or hired as an employee of the Financial Intelligence Unit, their identity may be ascertained and their personal data – including special-category data – may be processed, and information may be collected concerning the following:
1) the person's contact particulars, particulars of the person's residence, of the person's citizenship and identity document, of the person's employment and of the person's education history;
2) information concerning any sentence imposed on the person for an intentional criminal offence and concerning any previous convictions, information concerning the person's being released from their sentence and concerning the mandating of enforcement of their sentence;
3) information concerning criminal proceedings which have been instituted in respect of the person and in which the person has been declared the suspect or accused, and concerning any disposition by which proceedings have been terminated in these cases;
4) information concerning any sentence imposed on the person during the last five years for commission of any economic or financial misdemeanours, of misdemeanours relating to the person's office, of misdemeanours against public trust and of misdemeanours related to illegal handling of narcotic drugs and psychotropic substances, and for repeated commission of any other misdemeanours;
5) information concerning connections between the person and a criminal organisation or an organisation the aim of whose activities is the use of force to disrupt the sovereignty and independence of the Republic of Estonia, to violate its territorial integrity, to seize power or to change the constitutional order of Estonia;
6) information concerning any connections between the person and the intelligence or security services of a foreign state.

(2) A person who applies for the position of an official or of an employee of the Financial Intelligence Unit must fill out a personal information form as established by the Head of the Unit, in which they must provide information that allows to assess whether the person vetted is fit to be appointed as an official or hired as an employee. Among other matters, the form may require the person to provide information also in respect of their relatives by blood or marriage (parents, sisters, brothers, children, spouse and registered partner) and, in respect of a person with whom the respondent has a relationship similar to marriage, such a person's given names and surname as well as personal identity code or, where the person does not possess one, their date and place of birth. The information required in the form is preserved for five years following the person's application for the position of official or employee or following termination of their relationship of service or employment.
[RT I, 06.07.2023, 6 – entry into force 01.01.2024]

(3) In order to verify the information provided in the personal information form and to assess the person's fitness, the Head of the Financial Intelligence Unit or an official authorised by the Head has a right to:
1) address enquiries concerning personal particulars of the person vetted to authorities of the state and of local government, as well as to any natural or legal person;
2) interview the person vetted and any representative of their employer or educational institution, as well as any other persons, in order to ascertain the person' moral and other qualities and, where this is needed, to have the person provide a written explanation if they consent to do so;
3) verify whether the person vetted has been convicted of an intentionally committed criminal offence or of a misdemeanour that may cast doubt on the impeccability of their reputation, whether the person has been sentenced to imprisonment or whether they are the suspect or accused in criminal proceedings, including receiving information from the archive of the Criminal Records Database;
4) verify personal particulars against any database of the State, a local authority or another legal person in public law, or of a legal person in private law;
5) process any particulars concerning the person that are intended for the public and available from public sources.

(4) In order to collect information that is needed concerning any relatives by blood or marriage or concerning a person with whom the person vetted has a relationship similar to marriage, the Head of the Financial Intelligence Unit or an official authorised by the Head has a right to:
1) check the information contained in the database of the Unit;
2) check whether a sentence for an intentionally committed criminal offence whose particulars have not been removed from the Criminal Records Database has been imposed on such a person;
3) process any particulars concerning the person that are intended for the public and available from public sources.

(5) Any particulars or information mentioned in subsections 1 and 4 of this section may serve the Financial Intelligence Unit as grounds for refusing to appoint the person as an official or hire them as an employee. The reasons and the circumstances constituting grounds for the refusal are not disclosed.

(6) Where reasonable doubts arise regarding the presence of circumstances which would preclude appointing a person as an official or hiring them as an employee, the Financial Intelligence Unit may also verify the particulars or information mentioned in subsections 1 and 4 of this section concerning a person who has been appointed as an official or hired as an employee during the person's relationship of service or employment. Any circumstances that come to light in the course of assessing the fitness of a person during their relationship of service or employment may constitute grounds for discharging the person from service or terminating their contract of employment, provided these lead to the loss of confidence in the person, or would have precluded the person's being appointed as an official or hired as an employee.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

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

[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(1) The Financial Intelligence Unit and the Internal Security Service cooperate in investigation of transactions suspected of terrorist financing through mutual official assistance and exchange of information.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) The Director General of the Internal Security Service appoints a compliance officer who, on a footing equal to that of an official or employee of the Financial Intelligence Unit, has a right to receive information on any and all reports of suspicion of terrorist financing and, where this is needed, to make proposals for requiring additional information to be provided.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(3) The compliance officer of the Internal Security Service participates in the performance of the duties provided by clauses 1, 4, 6 and 7 of subsection 1 of § 54 of this Act and their authority and powers are governed by the provisions of subsections 1–$5^2$of § 60 and by § 61 of this Act as applicable to officials or employees of the Financial Intelligence Unit.
[RT I, 10.02.2023, 3 – entry into force 01.09.2023]

(4) The compliance officer of the Internal Security Service has a right to carry out regulatory enforcement duties provided by this Act jointly with an official or employee of the Financial Intelligence Unit.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 63. International exchange of information

(1) The Financial Intelligence Unit has a 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 or regulatory enforcement or supervisory agency as well as with an international organisation or institution.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(1^1) The Financial Intelligence Unit appoints an employee who is responsible for accepting requests for information sent by financial intelligence units located in other contracting states of the European Economic Area.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) The Financial Intelligence Unit has a 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(4) Upon implementation of subsections 2 and 3 of this section, the Financial Intelligence Unit uses only secure communication channels.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(5) Where 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 forwards the information thereon to the financial intelligence unit of the respective contracting state without delay.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(5^1) Where responding to a request for information received from the financial intelligence unit located in another contracting state of the European Economic Area calls for the acquisition of additional information from an obliged entity, the Financial Intelligence Unit acquires and forwards the information without delay.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(7^1) The Financial Intelligence Union may refuse to forward information to the financial intelligence unit of another contracting state of the European Economic Area only where the exchange of information is clearly outside the aims of AML/CFT or it might harm criminal proceedings or where the unit requesting information has not clarified 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(9) The Financial Intelligence Unit ensures that the consent to disseminate the information communicated based on a request is granted without delay 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(10) The Financial Intelligence Unit without delay grants the financial intelligence unit of another contracting state of the European Economic Area permission to disseminate the information communicated on the basis of the request to other competent authorities of the respective state. The permission may be refuses where the dissemination of information is clearly outside the AML/CFT aims or it would have criminal proceedings. The restriction of the dissemination of information is explained.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

Chapter 7
Enforcement, Supervisory and Oversight Arrangements

§ 64. Regulatory enforcement and supervisory authorities

(1) Unless otherwise provided by this section, the Financial Intelligence Unit acts as the regulatory enforcement authority in respect of the requirements arising from this Act and any legislation enacted under it.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) The Financial Supervision and Resolution Authority enforces compliance – 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 – with this Act and any legislation enacted under it. The Authority exercises supervision in accordance with the procedure provided for in the Financial Supervision Authority Act, without prejudice to special rules provided by this Act. The Authority exercises supervision over the credit institutions and financial institutions mentioned in the first sentence of this subsection in all areas of activity mentioned in § 2 of this Act and in the provision of the services mentioned in § 6.

(3) The Board of the Estonian Bar Association (hereinafter *Bar Association*) enforces compliance – by members of the Bar Association on the basis of the Bar Association Act – with this Act and any legislation enacted under it, having regard to the provisions of this Act.

(4) The Ministry of Justice enforces compliance with this Act and any legislation enacted under it 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 and Resolution 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.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(6) Regulatory enforcement and supervisory authorities have a right to exchange information and cooperate with their counterpart authorities of other countries based on the duties provided by this Act.

(7) Where this is needed, a regulatory enforcement or supervisory authority has a right to enlist the assistance of experts, interpreters and advisors in its enforcement or supervisory work, provided it is ensured that the person meets the requirements mentioned in subsection 1 of § 61 of this Act.

§ 65. Application of regulatory enforcement measures and imposition of non-compliance levies

(1) In order to carry out the regulatory enforcement work provided for in this Act, the Financial Intelligence Unit may apply special measures of regulatory enforcement provided by §§ 30–32, 35, 50 and 51 of the Law Enforcement Act, without prejudice to special rules provided by this Act.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) Where the obliged entity is a credit or financial institution, the maximum non-compliance levy in the event of failure to comply or of improper compliance with an administrative decision is:
1) in the case of a natural person, up to 5,000 euros on the first and up to 50,000 euros on any subsequent occasion in order to compel the person to perform one and the same duty or obligation, but not more than a total of 5,000,000 euros or the amount that corresponds to twice the benefit derived from the breach or twice the harm prevented;
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]
2) in the case of a legal person, up to 32,000 euros on the first and up to 100,000 euros on any subsequent occasion in order to compel the person to perform one and the same duty or obligation, but not more than the higher of 5,000,000 euros or up to 10 per cent of the person's total annual turnover according to the latest available annual accounts approved by its management body, or the amount that corresponds to twice the benefit derived from the breach or twice the harm prevented.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(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 compliance notice 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) Where persons not specified in subsections 2 and 3 of this section fail to comply with an administrative decision or improperly comply therewith, the maximum non-compliance levy is:
1) 5,000 euros in the case of a natural person;
2) up to 32,000 euros in the case of a legal person.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 66. Rights of administrative oversight authority

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

(2) In the event of an on-site inspection, the administrative oversight authority has a 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 any work processes;
2) receive oral and written explanations from the inspected obliged entity, members of its management body and employees.

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

§ 67. Duties of regulatory enforcement and supervisory authorities

(1) Where the Financial Supervision and Resolution Authority, the Board of the Bar Association, the Ministry of Justice or the Chamber of Notaries, in the course of regulatory enforcement work, identifies a situation whose characteristics give reason to suspect the presence of money laundering or terrorist financing, it notifies the Financial Intelligence Unit thereof without delay based on § 49 of this Act.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(1^1) If the Financial Supervision and Resolution Authority has, based on information or materials gathered in the course of financial supervision, above all, when assessing the organisation of the management, business model or activities of a credit institution or an investment firm, reasonable grounds to suspect that money has been or is being laundered or terrorism has been or is being financed in the credit institution or investment firm or that the credit institution or investment firm is involved in money laundering or terrorist financing or has committed an attempt thereof or there is a heightened risk of money laundering or terrorist financing in the credit institution or investment firm, the Financial Supervision and Resolution Authority informs the Financial Intelligence Unit and the European Banking Authority thereof without delay.

[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(1^2) In the event provided for in subsection 1 of this section, the Financial Supervision and Resolution Authority and the Financial Intelligence Unit cooperate to attend to the possible heightened risk of money laundering or terrorist financing and notify the European Banking Authority of their joint assessment without delay.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) The Financial Supervision and Resolution Authority, the board of the Bar Association and the Ministry of Justice must submit to the Financial Intelligence Unit by 15 April information about:
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]
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 Financial Intelligence Unit and the Financial Supervision and Resolution Authority publish on their websites without delay the final decision made in a misdemeanour case provided for in Chapter 10 of this Act or an administrative decision, compliance notice or decision to impose a non-compliance levy made in accordance with the procedure established in this Chapter after it has become final. At least the type and nature of the breach, the details of the person responsible for the breach and information on appealing against and setting aside of the decision or compliance notice is given on the website. The entire information must remain available on the website for at least five years.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(4) Upon assessment of the facts, the Financial Intelligence Unit and the Financial Supervision and Resolution Authority have a 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:
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]
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 Financial Intelligence Unit and the Financial Supervision and Resolution Authority have a 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 decision would be disproportionate in the case of a measure considered less important.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 68. Reporting of inspection results

(1) The Financial Supervision and Resolution 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 oversight 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 oversight authority and a copy thereof to the inspected person or its representative.

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

§ 69. Oversight of the work of the Financial Intelligence Unit

[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

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

[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) To assess the Financial Intelligence Unit's personal data processing process, the Data Protection Inspectorate has a 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 a right to receive data from the Financial Intelligence Unit to the extent required for making a decision on the complaint.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(3) Internal oversight over the lawfulness of the activities of the Financial Intelligence Unit is exercised by the minister in charge of the policy sector.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(4) The Financial Intelligence Unit is not subject to internal oversight as regards the performance of any tasks imposed on the Unit by this Act and the International Sanctions Act or the exercise of any rights provided for in the aforementioned legal instruments or the preparation and approval of any internal orders, instructions or records of the Unit in relation to the exercise of these rights, or any decisions concerning the service relationships of officials, or employment relationships of employees, of the Unit.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(5) [Repealed – RT I, 10.07.2020, 1 – entry into force 01.01.2021]

Chapter 8
Authorisation and Prohibition to Provide Services

[RT I, 10.07.2020, 1 - entry into force 20.07.2020]

§ 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) providers of trust and company services;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
3) providing pawnbroking services;
4) providing a virtual currency service;
[RT I, 31.12.2019, 2 – entry into force 10.03.2020]
5) [Repealed – RT I, 31.12.2019, 2 – entry into force 10.03.2020]
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 and Resolution Authority;
2) obligation to apply for the Financial Supervision and Resolution 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 and Resolution 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 § 20 of the International Sanctions Act, the rules of procedure and the procedure for verifying adherence thereto drawn up in accordance with § 23 of the International Sanctions Act;
[RT I, 19.03.2019, 11 – entry into force 01.01.2020]

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 3 of § 20 of the International Sanctions Act;
[RT I, 19.03.2019, 11 – entry into force 01.01.2020]
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 equivalent 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 intentionally 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;
9) where the undertaking, a member of its management body, procurator, beneficial owner or individual owner is a foreign citizen, copies of all of the identity documents of all of their countries of citizenship and the documents certifying the absence of the convictions, which are specified in clause 8 of this section;
[RT I, 31.12.2019, 2 – entry into force 10.03.2020
10) regarding a member of a management body and a procurator of the undertaking, documents indicating the level of education, a full list of the employers and jobs and, in the case of a member of a management body, also the field of responsibility, also documents that the applicant considers important to submit to prove the trustworthiness of the member of the management body or procurator and the fact that the applicant has a proper business reputation;
[RT I, 31.12.2019, 2 – entry into force 10.03.2020]
11) the list of payment accounts kept in the name of the undertaking, along with each payment account's unique feature and the account manager's name.
[RT I, 31.12.2019, 2 – entry into force 10.03.2020]

(3^1) Where the documents issued by the country specified in clause 8 or 9 of subsection 3 of this section do not prove the absence of a conviction to the required extent, such documents must be accompanied by a statement given under oath by the person the absence of whose conviction needs to be proven.
[RT I, 31.12.2019, 2 – entry into force 10.03.2020]

(3^2) In addition to the information required in the General Part of the Economic Activities Code Act, an application for authorisation concerning virtual currency operations must contain the following particulars and documents:
1) the amount of the assets and of share capital, as well as documents to prove that amount and the payment of the capital;
2) the applicant's initial balance sheet and an overview of its revenue, expenditure, profits and cash flows as well as the preconditions for these – or, for a going concern, the balance sheet and profit statement as of the end of the month preceding the filing of the application for authorisation and, if available, the annual reports for the last three years, unless these have been filed and made available in the databases maintained by the State;
3) a business plan that meets the requirements provided by § 70^1 of this Act;
4) documentation compiled in accordance with § 13 of this Act to ascertain the appetite for risk, and concerning risk analysis;
5) particulars concerning information technology systems and other technical means and systems required to provide the envisaged services, including a description of security measures used to ensure service resilience and protection of customers' assets, a description of measures to ensure business continuity and the level of technical organisation of operations;
6) a description of information technology systems and other technical means and systems which are to be used to provide the envisaged service and by which the service provider guarantees transmission of the particulars mentioned in subsections 2^4 and 2^5 of § 25 of this Act as well as identification of the customer and the customer's beneficial owners, the assignment of risk level to customers and the identification and monitoring of transactions and customers within the framework of a business relationship in a way that permits to meet the obligations provided by this Act and the special obligations provided by the International Sanctions Act, including identification of circumstances indicative of increased risk and suspicious transactions, and to notify these without delay;
7) the number of shares or votes held or to be acquired by each shareholder or member;
8) particulars of the audit undertaking retained by the applicant and of the applicant's internal auditor, including the name and personal identity code (where the person does not possess one, their date and place of birth) or registry code;
9) particulars of any persons who possess a significant holding in the applicant, including their name, personal identity code or, where they do not possess one, their date and place of birth, citizenship, residential address, employment position and contact particulars;
10) particulars concerning companies in which the holding of a member of the applicant's management body or of a person possessing a significant holding in the applicant exceeds 20 per cent, including – in respect of each company – its name, seat, registry code and the number of shares or votes held by a member of the applicant's management body or by a person possessing a significant holding in the applicant.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(4) In the case of an application for authorisation in a field specified in clause 1 or 4 of subsection1 of this section, the details specified in subsection 3 of this section must be accompanied by information on which financial service or virtual currency service will be provided.
[RT I, 31.12.2019, 2 – entry into force 10.03.2020]

(4^1) An authorisation for virtual currency operations cannot be assigned to another person.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(5) Where an undertaking wishes to use the authorisation also for the activities of a subsidiary, the undertaking files in respect of the subsidiary, in addition to the information required by the provisions of the General Part of the Economic Activities Code Act, all particulars and documents mentioned in subsection 3 and, where necessary, also those mentioned in subsections $3^2$and 4 of this section.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(6) The undertaking submits the applications, requests and notices related to the authorisation specified in subsection 1 of this section only via the Estonian information gateway or a notary in accordance with the single contact point principle.
[RT I, 31.12.2019, 2 – entry into force 10.03.2020]

§ 70^1. Virtual currency service provider's business plan

(1) The business plan of a provider of virtual currency service must set out the nature of the applicant's envisaged business activity, a description of its organisational and management structure, a description of the rights, obligations and responsibilities of persons related to providing the envisaged services, as well as a description, forecast and analysis of the following:
1) a magnitude of revenue and expenditure for each area of activity;
2) any obligations relating to provision of the service;
3) the amount of the applicant's assets and of its share capital;
4) its strategy, competitors and the market segment in which operations are envisaged;
5) its envisaged activities, services to be provided, products to be offered and prospective customers, including the proportion of customers who are Estonian residents and of those who are residents of other countries, as well as the volumes of envisaged services;
6) plans for its balance sheets and financial indicators which, among other things, mention revenues, expenditures, profits and cash flows as well as the preconditions for these;
7) general principles for risk management and a risk management strategy;
8) mediators and any other persons and services that will be used in the applicant's business activity;
9) any other material circumstances.

(2) A provider of virtual currency service files a business plan for at least two years.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 71. Granting of authorisation and refusal to grant authorisation

[RT I, 31.12.2019, 2 – entry into force 10.03.2020]

(1) Not later than within 60 working days following the date on which the application for authorisation was filed, the Financial Intelligence Unit disposes of the application by granting or refusing to grant the authorisation. The time limit for disposing of the application starts to run from the filing of all required documents and particulars. By decision of the Unit, the time limit for granting the authorisation may be extended to up to 120 days. Where the Unit has not disposed of the application within the time limit, the authorisation is not deemed to have been granted by default.

(2) If the undertaking who filed the application for authorisation has not produced all of the particulars and documents mentioned in § 70 of this Act or if such particulars and documents are incorrect or misleading or have not been presented in the required form, the Financial Intelligence Unit dismisses the application.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 72. Scope of scrutiny for and grounds for refusing to grant the authorisation

[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(1) Authorisation is granted to an undertaking where:
1) the undertaking, a member of its management body, procurator, beneficial owner and owner do not have any unspent conviction for a criminal offence against the authority of the state, offence relating to money laundering or other intentionally committed criminal offence;
1^1) the persons specified in clause 1 of this subsection have a proper business reputation;

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 whose activities the authorisation sought in the name of the undertaking is to be used for meets the requirements specified in clauses 1 and 2 of this section;
4) the registered seat, the seat of the management board and place of business of the undertaking applying for authorisation in the field of activity specified in clause 4 of subsection 1 of § 70 of this Act is in Estonia or a foreign company operates in Estonia via a branch that is registered in the commercial register and the place of business and the seat of the head of which is Estonia;
5) a payment account has been opened for the undertaking applying for authorisation in the field of activity specified in clause 4 of subsection 1 of § 70 of this Act in a credit institution, e-money institution or payment institution that has been established in Estonia or in a contracting state of the European Economic Area and provides cross-border services in Estonia or has established a branch in Estonia;
6) [Repealed – RT I, 12.03.2022, 2 – entry into force 15.03.2022]
7) an undertaking who applies for authorisation in the area of activity mentioned in clause 4 of subsection 1 of § 70 of this Act must meet the requirements provided by §§ 72^1–72^5.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(1^1) The Financial Intelligence Unit has a right to refuse to grant an authorisation for virtual currency operations where:
1) a significant connection between the undertaking and another person hampers adequate enforcement or supervision in respect of the applicant, or where such enforcement or supervision is hampered by requirements emanating from the legislation of another country in which the person with whom the applicant has a significant connection was founded – or is hampered due to the application of such requirements;
2) the information filed by the undertaking shows that it does not intend to operate in Estonia or its business has no connection to Estonia or – apart from a place of business and members of the management board who are in Estonia – its business has no significant connection to Estonia;
3) the internal rules filed by the undertaking are not adequate, proportionate or unambiguous considering the nature, scope and degree of complexity of the applicant's activities, or are contrary to applicable law;
4) the undertaking's information technology systems or other technical means are insufficient to provide the service;
5) there is reason to doubt whether the share capital's origin is legal;
6) an authorisation has previously been issued to the undertaking or a person with a significant holding in the undertaking, which has been revoked under clause 2, 4, 7, 8 or 9 of subsection 1 or clause 1, 2, 3, 4, 5, 6, or 7 of subsection 2 of § 75 of this Act or under clause 1 or 3 of subsection 1 or clause 2 or 3 of subsection 2 of 37 of the General Part of the Code of Economic Activities Act.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(2) A person is deemed not to possess a proper business reputation if the Financial Intelligence Unit has ascertained facts that cast doubt on the presence of such reputation or confirm its absence. A person does not possess a proper business reputation, among other things, when:
1) the person's actions or omissions have led to the bankruptcy of an undertaking or another person subject to financial supervision, or to revocation of an undertaking's or another person's authorisation on the motion of a financial supervision authority;
2) the person has committed a criminal offence of the first degree;
3) a court has imposed on the person a disqualification from certain professional activities under § 49 or an entrepreneurial disqualification under § 49^1 of the Penal Code, or the person is subject to an interim entrepreneurial disqualification or to a disqualification from working in a certain specialisation or holding a certain position, or the person has been sanctioned for violating such a disqualification;
4) the person is unable to organise the work of the undertaking such that the interests of investors and customers would enjoy sufficient protection;
5) the person has filed false information with the Unit, or has failed to file material information;
6) the person has been sentenced for an economic offence, for an offence relating to public office, for an offence against property or for an offence against public trust, or for a terrorist criminal offence or for having financed or assisted activities aimed at committing such a criminal offence, and the particulars of the corresponding conviction have not been removed from the Criminal Records Database in accordance with the Criminal Records Database Act, or an international sanction has been imposed on the person.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(3) The applicant for an authorisation for virtual currency operations, any member of the applicant's management body or any person with a significant holding in the applicant may not file a new application for authorisation during two years following the entry into effect of a decision by which the Financial Intelligence Unit refused to grant the authorisation, or by which the authorisation was revoked under clause 2, 4, 7, 8 or 9 of subsection 1 or clause 1, 2, 3, 4, 5, 6, or 7 of subsection 2 of § 75 of this Act or under clause 1 or 3 of subsection 1 or clause 2 or 3 of subsection 2 of 37 of the General Part of the Code of Economic Activities Act.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 72^1. Share capital of a provider of virtual currency service

(1) The share capital of a provider of virtual currency service must be:
1) at least 100,000 euros – where it provides one or several of the services mentioned in clauses 10, 10^1 or 10^3 of § 3 of this Act;

2) at least 250,000 euros – where it provides the service mentioned in clause 10^2 of § 3 of this Act.

(2) Where a provider of virtual currency service is established as a new company, only monetary contributions may be made to its share capital.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 72^2. Requirements for own funds of a provider of virtual currency service

(1) The own funds of a provider of virtual currency service must, at all times, correspond to one of the following magnitudes, depending on which of these is the larger:
1) the amount of the share capital as provided for by subsection 1 of § 72^1 of this Act;
2) the amount of own funds calculated according to the calculation method provided by subsections 3 or 6 of this section.

(2) The own funds of a provider of virtual currency service consist of common equity Tier 1 capital provided for by Articles 26–30 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), together with any deductions provided for by Article 36 of that Regulation – but without applying the exceptions related to the threshold provided by Articles 46 and 48 of that Regulation to those deductions.

(3) Where a provider of virtual currency service only provides the service mentioned in clause 10 or clause 10^3 of § 3 of this Act, the provider's own funds must not be less than 25 per cent of the fixed overhead costs of the previous financial year. Overhead costs are reviewed each year.

(4) Where a provider of virtual currency services has operated for less than 12 months, it may calculate fixed overhead costs by using estimates of business activity, provided it switches to data concerning previous periods as soon as those data become available.

(5) The principles for calculating fixed overhead costs for a financial year are enacted by a regulation of the Minister in charge of the policy sector.

(6) If a provider of virtual currency service only provides the service mentioned in clause 10^1 or clause 10^2 of § 3 of this Act, its own funds must at least be equal to the sum of the following part-volumes:
1) 4 per cent of the volume – which is less than or equal to 5,000,000 euros – of transactions carried out in the framework of provision of the service;
2) 2.5 per cent of the volume – which is higher than 5,000,000 euros but does not exceed 10,000,000 euros – of transactions carried out in the framework of provision of the service;
3) 1 per cent of the volume – which is higher than 10,000,000 euros but does not exceed 100,000,000 euros – of transactions carried out in the framework of provision of the service;
4) 0.5 per cent of the volume – which is higher than 100,000,000 euros but does not exceed 250,000,000 euros – of transactions carried out in the framework of provision of the service;
5) 0.25 per cent of the volume – which is higher than 250,000,000 euros – of transactions carried out in the framework of provision of the service.

(7) The basis for calculating the part-volume of transactions carried out in the framework of provision of the service mentioned in subsection 6 of this section is one twelfth of the total amount of the transfer and exchange transactions carried out by the provider of virtual currency service during the preceding year as services mentioned in clauses 10^1 and 10^2 of § 3 of this Act. A provider who, in the preceding year, has operated less than 12 months, obtains the relevant figure by dividing the sum of the volumes of transfer and exchange transactions carried out in the preceding year by the number of months of operation.

(8) A provider of virtual currency service is obligated to implement measures that permit, at any time, to calculate its own funds with sufficient precision.

(9) The Financial Intelligence Unit may set a time limit during which the provider of virtual currency service must take steps to ensure that its own funds meet the requirements provided by this Act and the legislation enacted under it.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 72^3. Auditing of providers of virtual currency service

(1) It is mandatory for the annual accounts of a provider of virtual currency service to be audited.

(2) Only a person mentioned in subsection 2 of § 7 of the Auditors' Activities Act may be appointed as an audit firm.

(3) An audit firm for a provider of virtual currency service may not be appointed for more than five years. It is not allowed to appoint an audit firm that has been appointed for five years for the directly following period.

(4) The audit firm must verify, as of the balance sheet date, compliance by the provider of virtual currency service with the requirements established in respect of its own funds, and present, by the due date of filing the provider's annual accounts, the corresponding opinion to the provider and to the Financial Intelligence Unit.

(5) The Financial Intelligence Unit has a right to require a provider of virtual currency service to appoint an audit firm where:
1) the general meeting of shareholders or the management board of the private limited company has not appointed an audit firm;
2) the audit firm that was appointed by the general meeting of shareholders or the management board of the private limited company has resigned its auditing duties;
3) in the view of the Financial Intelligence Unit, the audit firm has become untrustworthy.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 72[4]. Internal control and preservation of data

(1) A provider of virtual currency service must implement adequate measure of internal control that cover all of the provider's management and operational levels. for the annual accounts of a provider of virtual currency service to be audited.

(2) The supervisory board of a provider of virtual currency service appoints an internal auditor to perform the tasks of the internal control unit. An internal auditor is subject to the requirements and the legal basis provided by the Auditors' Activities Act in respect of certified internal auditors. An internal auditor may not undertake tasks which cause, may cause, a conflict of interests.

(3) The task of an internal auditor is to verify whether the operations of the provider of virtual currency service and of its managers comply with the requirements established by legislation, with any compliance notices issued by the Financial Intelligence Unit, with the decisions of the provider's management bodies, with internal rules, with the agreements concluded by the provider and with best practice.

(4) A provider of virtual currency service ensures that the internal auditor enjoys all rights and working conditions required for them to perform their duties, including the right to be provided explanations and information by the provider's managers and employees, and to monitor the elimination of any defects that have been discovered and the implementation of any proposals that have been made.

(5) An internal auditor is obligated to transmit, in writing, to the managers of the provider of virtual currency service and to the Financial Intelligence Unit, any information concerning the provider that the auditor has become privy to and that suggests a breach of the law or the harming of the interests of customers.

(6) A provider of virtual currency service and any of the provider's foreign branches preserve any information provided for in this Act unchanged and available to the Financial Intelligence Unit for five years following termination of business relationship with the customer, unless the Unit has, by compliance notice, established a different time limit, or the law provides a longer time limit.

(7) A provider of virtual currency service and any of the provider's branches preserve documents which lay down – in accordance with the agreement on provision of the service – the rights and obligations of the provider and of the customer, or the conditions under which the service is provided to the customer, for as long as the contractual or any other relationship relating to the provision of virtual currency service persists, unless a longer time limit is provided by this Act or other legislation.

(8) [Repealed – RT I, 21.06.2024, 3 – entry into force 01.07.2024]

§ 72[5]. Heightened requirements in respect of the seat, place of business, members of the management board and compliance officer of providers of virtual currency service

(1) Members of the management board of a provider of virtual currency service must possess a higher education and at leat two-year specialised work experience.

(2) A member of the management board of a provider of virtual currency service may not hold the position of member of the management board in more than two providers of virtual currency service.

(3) For the purposes of the restriction provided by subsection 2 of this section, the following positions are deemed to coincide:
1) positions of member of the management board within the same group;
2) positions of member of the management board in a company in which the provider of virtual currency service has a significant holding.

(4) The Financial Intelligence Unit may, in addition to those mentioned in subsection 2 of this section, grant permission to a member of the management board to accept one additional position of member of the management board.

(5) A compliance officer appointed by a provider of virtual currency service under § 17 of this Act may not hold the position of compliance officer or Head of unit in another provider of virtual currency service.

(6) A member of the management board of a provider of virtual currency service may only work as a compliance officer or Head of the corresponding unit in a provider of virtual currency service in which they are a member of the management board.

(7) The place of business of a provider of virtual currency service must make it possible to provide that service and to ensure, at any time, access for representatives of a regulatory enforcement or supervisory or investigative authority to the information that is collected and preserved.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 72[6]. Temporary ceasing of economic activities by a provider of virtual currency service

A provider of virtual currency service may not file, under subsection 2 of § 34 of the General Part of the Code of Economic Activities Act, a notice on temporary ceasing of economic activities.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 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 § 15 of the General Part of the Economic Activities Code Act.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 75. Revocation of authorisation

(1) 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 an authorisation mentioned in subsection 1 of § 70 of this Act where:
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]
1) the authorisation was granted to the undertaking by the Financial Supervision and Resolution Authority;
2) the undertaking repeatedly fails to follow compliance notices issued by a regulatory enforcement or supervisory authority;
3) the undertaking has not commenced operation in the requested area of activity within six months following issue of the authorisation;
4) the undertaking does not comply with the applicable conditions for granting an authorisation and the non-compliance has not been eliminated within the time limit – which must not be shorter than 30 days – granted for this purpose in the compliance notice;
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]
5) the operations of the provider of virtual currency service have been halted for more than six consecutive months;
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]
6) the provider of virtual currency service participates in the founding of a new company, or merges with another company, with its business being continued by the other company;
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]
7) the provider of virtual currency service has filed false information with the Financial Intelligence Unit, or such information has been filed on an authorisation granted by the provider;
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]
8) the provider of virtual currency service, a member of its management body, its procurator, beneficial owner or owner has been sentenced for an economic offence, for an offence relating to public office, for an offence against property or for an offence against public trust, or for a terrorist criminal offence or for having financed or assisted activities aimed at committing such a criminal offence, and the particulars of the corresponding conviction have not been removed from the Criminal Records Database in accordance with the Criminal Records Database Act;
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

9) the provider of virtual currency service, a member of its management body, its procurator, beneficial owner or owner has violated an international sanction or is in breach of the rules enacted by legislative instruments establishing such a sanction.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(2) In addition to the grounds provided by subsection 2 of § 37 of the General Part of the Code of Economic Activities Act and in subsection 1 of this section, the Financial Intelligence Unit may revoke an authorisation mentioned in clause 4 of subsection 1 of § 70 of this Act where:
1) the provider of virtual currency service is part of a consolidation group whose structure does not allow to obtain information thata is required for consolidated supervision, or where a company that is part of the same consolidation group as the provider has been founded in a state in which the competent supervisory authority does not have a legal basis or the possibility to engage in cooperation with the Financial Intelligence Unit, or where the requirements established by such a state's legislation, or their application, would interfere with the exercise of adequate supervision in respect of the applicant;
2) there is a significant connection between the provider of virtual currency service and another person, which interferes with the exercise of adequate supervision;
3) it comes to light that the provider of virtual currency service has selected Estonia as the place to apply for authorisation and registration in order to evade having to comply with the prohibitions or more stringent requirements applicable to the provider or the activity in the foreign state in which it conducts its principal business;
4) according to the information presented to the Financial Intelligence Unit by the competent regulatory enforcement or supervisory authority of a state party to the Agreement on the European Economic Area or of a third country, the provider of virtual currency service has violated the conditions established by a legislative instrument of such a state party or third country;
5) the provider of virtual currency service publishes, in respect of its activity or managers, information or advertisements that are materially incorrect or misleading;
6) the amount of the own funds of the provider of virtual currency service does not meet the requirements established by this Act or the legislation enacted under it;
7) the provider of virtual currency service has repeatedly, or to a material extent, violated the provisions of the legislation governing its activities.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 75[1]. Prohibition to provide services

An undertaking which – or whose supervisory board or management board member or beneficial owner – has an unspent conviction for an economic criminal offence or a criminal offence against property, against the State or against public trust is not allowed to provide services in the areas mentioned in clauses 4, 4[1], 7 and 8 of subsection 1 of § 2 of this Act.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

Chapter 9
Data of the Beneficial Owner of a Legal Person, of a Trust and of a Liability Account

[RT I, 02.06.2021, 1 - entry into force 07.03.2022]

§ 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 the owner's right of ownership or methods of exercising control. The data of the beneficial owner are kept by the management board of the private legal person in the Database of Beneficial Owners.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(1[1]) [Repealed – RT I, 02.06.2021, 1 – entry into force 12.06.2021]

(1[2]) A provider of trust services whose residence or registered seat is in Estonia is obligated to gather and keep with the Commercial Registry data concerning the persons mentioned in clauses 1–5 of subsection 6 of § 9 of this Act.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(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 methods 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;
5) a branch.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 76[1]. Database of Beneficial Owners

[Repealed – RT I, 02.06.2021, 1 – entry into force 12.06.2021]

§ 76[2]. Beneficial Ownership Information Database

(1) The Beneficial Ownership Information Database is established and its constitutive regulations are enacted by a regulation of the Minister in charge of the policy sector.

(2) The Ministry of Finance is the controller of the Beneficial Ownership Information Database. The processors of the Database are the Centre of Registers and Information Systems and the Registry Department of Tartu District Court (hereinafter *Registry Department*).

(3) The Beneficial Ownership Information Database stores particulars that have been filed under § 77 as well as information on notes that have been recorded under § 77[2] of this Act.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(4) The data in the Beneficial Ownership Information Database are provided for information purposes.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 77. Submission of data

(1) Following the provisions of subsections 2–4[2] of § 9 and § 76 of this Act, a general partnership, limited partnership, private limited company, public limited company or commercial association files with the Beneficial Ownership Information Database – 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 that code (upon absence of a personal identification code, the date and place of birth), and the country of residence;
2) data on the method by which the person exercises control.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(1[1]) [Repealed – RT I, 02.06.2021, 1 – entry into force 12.06.2021]

(1[2]) [Repealed – RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(2) Following the provisions of subsection 7 of § 9 of this Act, a non-profit association files with the Beneficial Ownership Information Database – 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 that code (upon absence of a personal identification code, the date and place of birth), and the country of residence;
2) data on the method by which the person exercises control.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(3) Following the provisions of subsection 7 of § 9 of this Act, a foundation files with the Beneficial Ownership Information Database – 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 that code (upon absence of a personal identification code, the date and place of birth), and the country of residence;
2) data on the method by which the person exercises control;
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 that 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.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(3[1]) [Repealed – RT I, 02.06.2021, 1 – entry into force 12.06.2021]

(3[2]) [Repealed – RT I, 02.06.2021, 1 – entry into force 12.06.2021]

(3^3) A provider of trust services files with the Beneficial Ownership Information Database via the Commercial Register information system – in respect of the persons mentioned in clauses 1–5 of subsection 6 of § 9 of this Act – the person's name, their identification code or registration number and the country of that code or number (or, where a person does not possess a personal identification code, the date and place of birth and the country of residence).
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(3^4) A provider of trust services also files with the Beneficial Ownership Information Database via the Commercial Register information system the full name of the trust, the date of its creation, the name of the country under whose law the trust was created, as well as the provider's own address, telephone number and email address.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

(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.

(4^1) [Repealed – RT I, 02.06.2021, 1 – entry into force 12.06.2021]

(4^2) A provider of trust services files the data specified in subsections $3^3$and $3^4$of this section within 30 days following:
1) the creation of the trust;
2) their becoming the trustee or
3) their obtaining a temprorary right of residence.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(5) In a situation where there is a change in the data that have been filed, the company, non-profit association or foundation files the new data within 30 days of learning of the change.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(6) Where the data of the beneficial owner remain unchanged, the company, non-profit association or foundation certifies the correctness of the data upon submission of the annual report.
[RT I, 17.11.2017, 2 – entry into force 01.09.2018]

§ 77^1. Ensuring correctness of data

[Repealed – RT I, 02.06.2021, 1 – entry into force 12.06.2021]

§ 77^2. Ensuring correctness of data

(1) Where a person who is obligated under § 77 of this Act to file certain data has not complied with the obligation provided by that section, the Registry Department notifies this to the person and demands the filing of the data.

(2) The person must file the data within 10 days of receiving the notification mentioned in subsection 1 of this section.

(3) Where the Registry Department receives a notification concerning incorrectness of beneficial owners' data that is made under subsection $2^4$of § 20 of this Act and is duly substantiated, it notifies this to the person obligated to file those data and records a note with the data stating that there are doubts concerning their accuracy.

(4) A note mentioned in subsection 3 of this section is automatically removed when the correctness of the data has been confirmed or the data have been changed.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

§ 78. Publication of data

(1) The data of the beneficial owner and any notes recorded concerning those data are made public in the Commercial Register information system.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

(2) The fees for issuing the data of a beneficial owner are established by a regulation of the minister in charge of the policy sector.

(3) The data of the beneficial owner are issued free of charge to the obliged entity, a government agency, the Financial Supervision and Resolution Authority and to a court.
[RT I, 17.11.2017, 2 – entry into force 01.09.2018]

§ 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 a 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.
[RT I, 17.11.2017, 2 – entry into force 01.09.2018]

§ 79[1]. Beneficial owner's right to demand limitation of access to submitted data

[Repealed – RT I, 02.06.2021, 1 – entry into force 12.06.2021]

§ 79[2]. Beneficial owner's right to demand limitation of access to submitted data

(1) In a situation where public access to the data of a beneficial owner would expose such an owner to a disproportionately high risk of fraud, kidnapping, blackmail, extortion, harassment, violence or intimidation, the beneficial owner and their representative have a right to apply to the processor of the register for a limitation of access to the data in exceptional circumstances.

(2) Where the beneficial owner is a minor or a person of limited active legal capacity, their representative may apply for a limitation of public access to the data until the beneficial owner is of full age or until they regain their active legal capacity.

(3) On a substantiated application of the beneficial owner or their representative, the controller of the Beneficial Owner Information Database limits the public's access to the data, provided the presence of circumstances mentioned in subsections 1 and 2 of this section has been proven. The limitation is removed when the circumstance that constitutes grounds for limiting the access is no longer present. The controller of the Database notifies the applicant of the decision to grant or deny an application for limiting the public's access to data, and of the decision to remove the limitation.

(4) Where access to certain data has been limited under subsections 1 or 2 of this section, such data are only disclosed to a credit or financial insitution, a notary, an authority of the executive branch of government, the Financial Supervision and Resolution Authority or the Financial Intelligence Unit.

(5) The controller of the Beneficial Owner Information Database presents an overview concerning the number of and reasons for decisions taken under subsection 3 of this section to the European Commission.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 80. Deletion of data

(1) The data of the beneficial owner are deleted automatically five years after deletion of the legal person from the register.
[RT I, 17.11.2017, 2 – entry into force 01.09.2018]

(2) [Repealed – RT I, 02.06.2021, 1 – entry into force 12.06.2021]

(3) The Registrar deletes the data of a beneficial owner of a trust if the person who has a legitimate interest in the deletion proves that at least five years have elapsed since the circumstance that triggered the filing of those data ceased to apply.
[RT I, 02.06.2021, 1 – entry into force 07.03.2022]

§ 81. Mandatoriness of automated communication of liability account information

(1) A credit institution or a financial institution that has opened for a customer a payment account (hereinafter *account*) that has an International Bank Account Number (IBAN) or let them a safe-deposit box must ensure that at least the particulars mentioned in subsections 1^1–$1^5$of this section are available via the Enforcement Register mentioned in § 63 of the Code of Enforcement Procedure.
[RT I, 09.04.2021, 1 – entry into force 01.01.2024]

(1^1) The following is made available regarding an account holder and a safe-deposit box lessee:
1) name;
2) personal identification code and the state that issued it or, upon absence thereof, the date and state of birth or the registry code;
3) postal address.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(1^2) The following is made available on a person authorised to use an account:
1) name;
2) personal identification code and the state that issued it or, upon absence thereof, the date and state of birth;
3) postal address;
4) the date of the beginning and end of the authorisation and the substance of the right of use.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(1^3) The following is made available regarding the beneficial owner of an account holder:
1) name;
2) personal identification code and the state that issued it or, upon absence thereof, the date and state of birth;
3) the country of residence.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(1^4) The following is made available regarding an account:
1) IBAN;
2) the date of opening the account;
3) the date of closing the account.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(1^5) With respect to a safe-deposit box, the following particulars of the contract for its use are made available:
1) contract number;
2) date of conclusion;
3) date of termination.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2) For the purposes of this section, IBAN (International Bank Account Number) means an international account feature that complies with the EVS 876:2016 standard and whose elements have been determined by the International Organization for Standardization and that uniquely identifies an individual account in a Member State.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(3) The availability of the details specified in subsections 1^1, $1^4$and $1^5$is ensured regarding an existing account and a valid safe-deposit box contract as well as an account closed and a contract of use of a safe-deposit box terminated during a five-year period preceding the receipt of an inquiry.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(4) The availability of the details specified in subsection $1^2$of this section is in the case of an existing account ensured regarding a five-year period preceding the receipt of an inquiry.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(5) The availability of the details specified in subsection $1^3$of this section is in the case of an existing account ensured as of the moment of responding to the inquiry.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

Chapter 10
Liability

§ 82. Violation of, and failure to implement, requirements established concerning money laundering and terrorist financing risk assessment, procedural rules and internal control rules

[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(1) The penalty for violating requirements established concerning risk assessment by § 13 of this Act or concerning procedural rules or internal control rules by § 14 of this Act, or for failure to implement the procedural rules or internal control rules, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(2) The penalty for the same act, where the obliged entity was subject to financial supervision – mentioned in the Financial Supervision Authority Act – by the Financial Supervision and Resolution Authority is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(3) The penalty for the act provided for by subsection 1 of this section, where committed by a legal person, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(4) The penalty for the act provided for by subsection 2 of this section, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the

misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 83. Opening of anonymous account or savings book or safe-deposit box or virtual currency wallet or crypto-asset account

[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(1) The penalty for violating the prohibition – applicable to a credit or financial institution or a provider of virtual currency service by virtue of subsection 2 of § 25 of this Act – on making a decision to open an anonymous account, savings book, virtual currency wallet, crypto-asset account or safe-deposit box or concluding a corresponding contract is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(2) The penalty for the same act, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 84. Failure to perform the duty to identify the person and verify their identity

(1) The penalty for a breach by an obliged entity, its management board member or employee of the duty provided for by this Act to identify a customer or a person participating in an occasional transaction, or a person's representative, and to verify their identity, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(2) The penalty for the same act, where the obliged entity was subject to financial supervision – mentioned in the Financial Supervision Authority Act – by the Financial Supervision and Resolution Authority is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(3) The penalty for the act provided for by subsection 1 of this section, where committed by a legal person, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(4) The penalty for the act provided for by subsection 2 of this section, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 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 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(2) The penalty for the same act, where the obliged entity was subject to financial supervision – mentioned in the Financial Supervision Authority Act – by the Financial Supervision and Resolution Authority is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(3) The penalty for the act provided for by subsection 1 of this section, where committed by a legal person, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(4) The penalty for the act provided for by subsection 2 of this section, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 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 is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(2) The penalty for the same act, where the obliged entity was subject to financial supervision – mentioned in the Financial Supervision Authority Act – by the Financial Supervision and Resolution Authority is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(3) The penalty for the act provided for by subsection 1 of this section, where committed by a legal person, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(4) The penalty for the act provided for by subsection 2 of this section, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

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

(1) The penalty for a breach of the requirements for making a transaction with a politically exposed person is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(2) The penalty for the same act, where the obliged entity was subject to financial supervision – mentioned in the Financial Supervision Authority Act – by the Financial Supervision and Resolution Authority is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(3) The penalty for the act provided for by subsection 1 of this section, where committed by a legal person, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(4) The penalty for the act provided for by subsection 2 of this section, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 88. Violation of prohibition to establish a business relationship and make an 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 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(1^1) The penalty for the same act, where the obliged entity was subject to financial supervision – mentioned in the Financial Supervision Authority Act – by the Financial Supervision and Resolution Authority is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(2) The penalty for the act provided for by subsection 1 of this section, where committed by a legal person, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(3) The penalty for the act provided for by subsection 1^1 of this section, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 89. Breach of the duty to monitor a business relationship

(1) The penalty for a breach of the duty provided for by this Act to monitor a business relationship is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(2) The penalty for the same act, where the obliged entity was subject to financial supervision – mentioned in the Financial Supervision Authority Act – by the Financial Supervision and Resolution Authority is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(3) The penalty for the act provided for by subsection 1 of this section, where committed by a legal person, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(4) The penalty for the act provided for by subsection 2 of this section, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 90. Violation of prohibition to outsource activity

(1) The penalty for violating the prohibition provided by this Act on outsourcing an activity is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(2) The penalty for the same act, where the obliged entity was subject to financial supervision – mentioned in the Financial Supervision Authority Act – by the Financial Supervision and Resolution Authority is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(3) The penalty for the act provided for by subsection 1 of this section, where committed by a legal person, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(4) The penalty for the act provided for by subsection 2 of this section, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 91. Breach of correspondent communication requirements

[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(1) The penalty for establishing a correspondent relationship in breach of the requirements provided by this Act is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(2) The penalty for the same act, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 92. Breach of the duty to report a 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, or of a foreign exchange transaction or any other transaction by which a monetary obligation exceeding 32,000 euros or an equivalent sum in another currency is performed in cash is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(1^1) The penalty for the same act, where the obliged entity was subject to financial supervision – mentioned in the Financial Supervision Authority Act – by the Financial Supervision and Resolution Authority is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(2) The penalty for the same act, where committed by a legal person, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(3) The penalty for the act provided for by subsection 1[1] of this section, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

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

[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(1) The penalty for illegal notification of a person, their representative, the person's beneficial owner or the public by the obliged entity, its management board member, compliance officer or employee, or by an employee of a supervisory authority, concerning a report or data forwarded to, or a compliance notice issued by, the Financial Intelligence Unit regarding the person, or about the or about the institution of criminal proceedings against the person is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(1[1]) The penalty for the same act, where the obliged entity was subject to financial supervision – mentioned in the Financial Supervision Authority Act – by the Financial Supervision and Resolution Authority is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(2) The penalty for the act provided for by subsection 1 of this section, where committed by a legal person, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

(3) The penalty for the act provided for by subsection 1[1] of this section, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 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 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(2) The penalty for the same act, where the obliged entity was subject to financial supervision – mentioned in the Financial Supervision Authority Act – by the Financial Supervision and Resolution Authority is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(3) The penalty for the act provided for by subsection 1 of this section, where committed by a legal person, is a fine of up to 1,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.

(4) The penalty for the act provided for by subsection 2 of this section, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 94[1]. Violation of obligation to notify of change of circumstances relating to economic activities and termination of economic activities

(1) The penalty for a breach of the obligation to notify of a change of the circumstances relating to the object of inspection or the secondary conditions of the authorisation specified in subsection 1 of § 70 of this Act, the obligation of advance notification of the intention to change the aforementioned circumstance or the obligation to notify of the termination of the activities of a service provider is a fine of up to 300 fine units.

(2) The penalty for the same act, where committed by a legal person, is a fine of up to 400,000 euros.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 94[2]. Violation of prohibition to provide services

(1) The penalty for violation of the prohibition to provide a service specified in § 75[1] of this Act is a fine of up to 300 fine units.

(2) The penalty for the same act, where committed by a legal person, is a fine of up to 400,000 euros.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 94[3]. Violation of reporting obligation

(1) The penalty for violation of the reporting obligation established on the basis of § 54[1] of this Act is a fine of up to 300 fine units.

(2) The penalty for the same act, where committed by a legal person, is a fine of up to 400,000 euros.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 94[4]. Violation of requirements on own funds

(1) The penalty for violation of the requirements established by this Act or under it for the own funds of a provider of virtual currency service is a fine of up to 300 fine units.

(2) The penalty for the same act, where committed by a legal person, is a fine of up to 400,000 euros.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 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 or a trustee to submit the details of the beneficial owner or for failure to report on a change of the details or for knowingly submitting false information, where it has caused a situation where the obliged entity cannot apply the due diligence measure provided for by clause 3 of subsection 1 of § 20 of this Act has been caused, is a fine of up to 300 fine units.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(2) The penalty for the same act, where committed by a legal person, is a fine of up to 400,000 euros.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 96. Breach of obligations of providerofpayment service

(1) The penalty for failure, by an executive or employee of a provider of payment service – or by an executive or employment of a payment agent – to ascertain or verify, or transmit, any information relating to the payer, as well as for a breach of any other obligation of payment service providers as provided by Articles 4, 5, 6, 8, 11, 12 or 26 of Regulation (EU) No 2023/1113 of the European Parliament and of the Council, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(2) The penalty for the same act, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 96[1]. Breach of obligations of provider of virtual currency service

(1) The penalty for failure by an executive or employee of a provider of virtual currency service to ascertain or verify any information relating to a payer, or to forward such information, or for any other violation of obligations incumbent on or for providing the service outside of a business relationship – or for a breach of any other duties of providers of virtual currency service provided by § 25 of this Act – is a fine of up to 300 fine units.

(2) The penalty for the same act, where committed by a legal person, is a fine of up to 400,000 euros.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 96[2]. Breach of obligations of crypto-asset service provider

(1) The penalty for failure, by an executive or employee of a crypto-asset service provider to ascertain or verify, or transmit, any information relating to the originator of the transaction, as well as for a breach of any other obligation of the provider of virtual currency service as provided by Articles 14, 15, 17, 19, 20, 21 or 26 of Regulation (EU) No 2023/1113 of the European Parliament and of the Council, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

(2) The penalty for the same act, where committed by a legal person, is a fine of up to 5,000,000 euros or of up to twice the amount corresponding to the benefit derived from the misdemeanour or to the harm prevented, or of up to 10 per cent of the consolidated turnover of the legal person or of the person's consolidation group.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

§ 96[3]. Limitation period

[Repealed – RT I, 21.06.2024, 3 – entry into force 30.12.2024]

§ 96[4]. Turnover of legal person and of consolidation group

[RT I, 21.06.2024, 3 – entry into force 30.12.2024 – the section's number, 96[2], changed to 96[4]]
As provided for by this Chapter, the turnover of a legal person means the yearly total turnover according to the last available accounts approved by the person's management body. Where the legal person is a parent company, or a subsidiary of a parent that is required to draw up consolidated accounts, the total turnover mentioned in the first sentence means the total yearly turnover or the total turnover for the type of income concerned according to the last available accounts that have been approved by the management body of the highest-level parent company.
[RT I, 17.03.2023, 2 – entry into force 01.11.2023]

§ 97. Proceedings

(1) The Financial Intelligence Unit and the Financial Supervision and Resolution Authority are the out-of-court proceedings authorities regarding the misdemeanours provided for by this Chapter.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) The limitation period for the misdemeanours provided by §§ 82–94 and 96–96[2]of this Act is three years.
[RT I, 21.06.2024, 3 – entry into force 30.12.2024]

Chapter 11
Implementing Provisions

§ 98. Follow-up analysis of implementation of this 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*.

§ 98[1]. Transitional provisions concerning transformation of Financial Intelligence Unit into governmental authority

(1) As of 1 January 2021, the functions, rights and competence of the Financial Intelligence Unit which has operated as a structural unit of the Police and Border Guard Board (hereinafter in this section *PBGB FIU*) and those of its officials transfer to the Financial Intelligence Unit and its officials in the area of government of the Ministry of Finance.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(2) The legal succession specified in subsection 1 of this section also applies to participation in international organisations, cooperation agreements as well as to the access that the Financial Intelligence Unit and its officials have to all of the national registers, databases and information systems.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(3) Until 1 January 2021, the PBGB FIU continues to perform its functions, including to represent the Financial Intelligence Unit in international organisations, cooperation agreements, domestic organisations and proceedings.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(4) The information, case files, databases and data media at the disposal of and held by the PBGB FIU are handed over to the Financial Intelligence Unit in the area of government of the Ministry of Finance not later than on 1 January 2021.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(5) Administrative proceedings and supervision operations instituted on the basis of this Act or the International Sanctions Act before 1 January 2021, which continue after 1 January 2021 are completed by the Financial Intelligence Unit in the area of government of the Ministry of Finance.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(6) In the case of misdemeanour proceedings initiated by the PBGB FIU before 1 January 2021 on the basis of this Act and the International Sanctions Act, the out-of-court proceedings authority is, as of 1 January 2021, the Financial Intelligence Unit in the area of government of the Ministry of Finance.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(7) In the case of a complaint against an administrative decision or operation of the PBGB FIU filed with an administrative court before 1 January 2021 the Financial Intelligence Unit in the area of government of the Ministry of Finance is the party to the proceedings instead of the PBGB FIU as of 1 January 2021.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(8) The officials of the PBGB FIU whose functions and position do not change are transferred for an unspecified period to a position in the Financial Intelligence Unit in the area of government of the Ministry of Finance as of 1 January 2021 on the basis of clause 1 of subsection 1 of § 98 of the Civil Service Act.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(9) The police officers of the PBGB FIU whose functions and position do not change are, based on their written consent, released from police service and transferred for an unspecified period to a position in the Financial Intelligence Unit in the area of government of the Ministry of Finance as of 1 January 2021 on the basis of clause 1 of subsection 1 of § 98 of the Civil Service Act, taking into account the specifics of this section.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(10) As of 1 January 2021, the head of the PBGB FIU is transferred to the position of the head of the Financial Intelligence Unit in the area of government of the Ministry of Finance until the expiry of the time limit arising from a decree of the Director General of the Police and Border Guard Board by which they were appointed to office, applying the provisions of the Police and Border Guard Act. A public competition specified in subsection 2 of § 53 of the version of this Act that enters into force of 1 January 2021 for the appointment of the head of the Financial Intelligence Unit will be carried out by 15 October 2020.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(11) Upon transfer of a police officer based on subsections 9 and 10 of this section, the counting of their length of police service continues and they retain their right to a police officer's superannuated pension in accordance with § 111^1 of the Police and Board Guard Act, provided that they hold a position in the Financial Intelligence Unit in the area of government of the Ministry of Finance or in the police service.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

(12) The right of a police officer to a police officer's superannuated pension specified in subsection 11 of this Act does not depend on the length of police service immediately preceding the attainment of the retirement age or on retirement from the police service.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

(13) The Minister of Finance or a person authorised by the Minister of Finance makes administrative decisions, makes transactions and takes steps related to making the Financial Intelligence Unit of the Police and Border Guard Board a governmental agency in the area of government of the Ministry of Finance, including steps related to the transfer of officials and police officers.
[RT I, 21.11.2020, 1 – entry into force 23.11.2020]

§ 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 2,000 euros or an equivalent 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.

§ 100^1. Verification of details of beneficial owner

Obliged entities apply the due diligence measure specified in subsection 2^1 of § 20 of this Act to customers with whom they have established a lasting business relationship before the entry into force of this section, within one year after the entry into force of this section.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 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.

§ 104[1]. Application of prohibition to provide services

A person specified in § 75[1] of this Act who started providing the services specified in the same section before the entry into force of the section brings their activities into compliance with the requirements of the section not later than by 31 December 2020.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 104[2]. Ensuring access to data via electronic attachment system

Credit and financial institutions must perform the obligations specified in subsections 1, 3, 4 and 5 of § 81 of this Act as of 10 September 2020.
[RT I, 10.07.2020, 1 – entry into force 20.07.2020]

§ 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.–§ 112.[Omitted from this text.]

§ 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.]

§ 118[1]. Equivalence of authorisation of provider of virtual currency service

The authorisation of a provider of a service of exchanging a virtual currency against a fiat currency and the authorisation of a virtual currency wallet service provider granted on the basis of this Act is considered equivalent to the authorisation of a virtual currency service provider.

[RT I, 31.12.2019, 2 – entry into force 10.03.2020]

§ 118[2]. Bringing operations of undertakings holding a valid authorisation into compliance with the version of this Act adopted on 11 December 2019

(1) An undertaking that has been granted authorisation on the basis of this Act is required to bring its operations and documents into compliance with the requirements provided for in clauses 9–11 of subsection 3 of § 70 and clauses 1[1], 4, 5 and 6 of subsection 1 of § 72 of the version of this Act adopted on 11 December 2019 not later than by 1 July 2020.

(2) Where an undertaking fails to bring its operations into compliance with the law within the time limit set in subsection 1 and to submit the documents, the Financial Intelligence Unit revokes the undertaking's authorisation.
[RT I, 21.11.2020, 1 – entry into force 01.01.2021]

§ 118[3]. Bringing the operations of undertakings holding a valid authorisation into compliance with the version of this Act that entered into force on 15 March 2022

(1) A provider of virtual currency service who has been granted an authorisation under this Act is required, by 15 June 2022, to bring its operations and documents into compliance with subsection 3[2] of § 70, with §§ 72[1] and 72[2], with subsections 2–5 of § 72[3] and with §§ 72[4] and 72[5] of the version of this Act that entered into force on 15 March 2022.

(2) The audit obligation provided by subsection 1 of § 72[3] of this Act applies to the annual accounting periods of providers of virtual currency service that start on 10 March 2022 or later.

(3) A provider of virtual currency service that has been granted an authorisation under this Act is required to ensure that the opinion provided for in subsection 4 of § 72[3] of this Act is presented to the Financial Intelligence Unit by 1 January 2023 at the latest.

(4) If the provider of virtual currency service does not, within the time limit provided by subsection 1 of this section, bring their operations into compliance and file documents, the Financial Intelligence Unit revokes the authorisation granted in the area of virtual currency operations.

(5) The economic activities of all providers of virtual currency service who have filed a notice of temporary ceasing of such activities and who have not, by 15 March 2022, resumed those activities, are deemed to have been resumed as of 15 June 2022.

(6) In the context of bringing into compliance of the operations of an undertaking that holds a valid authorisation, proceedings on varying such an authorisation may be extended by the Financial Intelligence Unit up to 150 days.
[RT I, 12.03.2022, 2 – entry into force 15.03.2022]

§ 118[4]. Virtual currency service provider's authorisation

(1) Starting from 30 December 2024, an undertaking cannot, under his Act, apply for an authorisation to provide the virtual currency service, and cannot, starting from 1 July 2026, apply to amend such an authorisation.

(2) If the application for an virtual currency service provider's authorisation has been filed with the Financial Intelligence Unit before 30 December 2024 and the Unit has not granted the application by that date, it dismisses the application. Where the application is dismissed, the Unit returns the documents that have been filed.

(3) The virtual currency service provider's authorisation issued under this Act is deprived of effect under clause 1 of subsection 1 of § 75 of this Act where the undertaking has been issued, by the Estonian Financial Supervision and Resolution Authority, a crypto-asset service provider's authorisation under Regulation (EU) 2023/1114 of the European Parliament and of the Council or, at the latest, on 1 July 2026.
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

§ 118[5]. Special rule for audits of own funds of providers of virtual currency service

Subsection 4 of § 72[3] of this Act is not applied where the authorisation of the virtual currency service provider has been deprived of effect on the condition provided by subsection 3 of § 118[4].
[RT I, 21.06.2024, 3 – entry into force 01.07.2024]

§ 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), amended by Directives (EU) 2018/843 (OJ L 156, 19.06.2018, pp. 43–74) and (EU) 2019/2177 (OJ L 334, 27.12.2019, pp. 155–163); Directive 2011/16/EU of the Council on administrative cooperation in the field of taxation and repealing Directive 77/799/EEC (OJ L 64, 11.03.2011, pp. 1–12), amended by Directives 2014/107/EU (OJ L 359, 16.12.2014, pp. 1–29), (EU) 2015/2376 (OJ L 332, 18.12.2015, pp. 1–10), (EU) 2016/881 (OJ L 146, 03.06.2016, pp. 8–21), (EU) 2016/2258 (OJ L 342, 16.12.2016, pp. 1–3), (EU) 2018/822 (OJ L 139, 05.06.2018, pp. 1–13), (EU) 2020/876 (OJ L 204, 26.06.2020, pp. 46–48) and (EU) 2021/514 (OJ L 104, 25.03.2021, pp. 1–26); Directive (EU) 2019/1153 of the European Parliament and of the Council laying down rules for facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA (OJ L 186, 11.07.2019, pp. 122–137) [RT I, 12.03.2022, 2 – entry into force 15.03.2022]