

Issuer: Riigikogu
Type: act
In force from: 01.01.2026
In force until: In force
Translation published: 28.01.2026

Cybersecurity Act¹

Passed 09.05.2018

RT I, 22.05.2018, 1

Entry into force 23.05.2018, in part 01.01.2020 and 01.01.2022

Amended by the following acts

Passed	Published	Entry into force
19.07.2022	RT I, 06.08.2022, 2	16.08.2022, in part 01.01.2027; amended in part [RT I, 30.12.2025, 4]
04.06.2024	RT I, 21.06.2024, 2	01.07.2024
10.12.2025	RT I, 30.12.2025, 4	01.01.2026

Chapter 1 General Provisions

§ 1. Scope of regulation and scope of application of Act

(1) This Act provides for:

- 1) requirements for the maintenance of the network and information systems used by essential entities and important entities and domain name registration service providers, as well as liability and supervision;
- 2) grounds for handling cyber incidents and requirements for addressing security vulnerabilities and cyber threats;
- 3) requirements for preventing and responding to large-scale cyber incidents and crises;
- 4) requirements for co-operation, information sharing and peer review in the field of cybersecurity;
- 5) the competent authorities in the field of cybersecurity and the requirements for designating the competent authority carrying out cybersecurity supervision in the field of cross-border electricity flows.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(2) This Act is not applied to:

- 1) the processing of state secrets and classified information of foreign states or to the maintenance of processing systems for such information;
- 2) the maintenance of systems necessary for international military co-operation and for preparations for national military defence within the area of government of the Ministry of Defence;
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]
- 3) the diplomatic and consular missions of the Republic of Estonia in third countries and their network and information systems, where such systems are located on the premises of the mission or are operated for users in a third country.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(2¹) The exemption provided in subsection 2 of this section does not apply to a trust service provider.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(3) [Repealed – RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(4) Where the requirements for the maintenance of a service provider's network and information system and for the notification of a cyber incident are governed by an international agreement, a European Union legal act or another Act in a manner equivalent to that provided in this Act, this Act is applied with the specifications arising from the international agreement, European Union legal act or other Act.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

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

§ 2. Definitions

For the purposes of this Act, definitions have the following meanings:

- 1) 'data centre service' means a service that encompasses structures, or groups of structures, dedicated to the centralised accommodation, interconnection and operation of information technology and network equipment providing data storage, processing and transport services, including all the facilities and infrastructures for power supply and accommodation environment control;
- 2) 'digital service provider' means a generic term referring to a domain name system service provider, a top-level domain name registry, a domain name registration service provider, a cloud computing service provider, a data centre service provider, a content delivery network service provider, a managed service provider, an information security service provider, an online marketplace provider and a provider of an online search engine or a social media platform;
- 3) 'representative of a digital service provider' (hereinafter *representative*) means a natural or legal person established in the European Union designated to act on behalf of a digital service provider not established in the European Union, which may be addressed by the Estonian Information System Authority with regard to the obligations of the digital service provider;
- 4) 'domain name registration service provider' means a top-level domain name registry or a person acting on behalf of that top-level domain name registry, such as a privacy or proxy registration service provider or a reseller;
- 5) 'domain name system' means a hierarchical and distributed naming system which enables the identification of internet services and resources by making it possible for end-user devices to use internet routing and connectivity services to reach those services and resources;
- 6) 'domain name system service provider' means an entity that provides publicly available recursive domain name resolution services for internet end-users, or that provides authoritative domain name resolution services for third-party use, with the exception of root name servers;
- 7) 'managed service provider' means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely;
- 8) 'ICT process' means an ICT process as defined in point 14 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 07.06.2019, pp 15–69);
- 9) 'ICT service' means an ICT service as defined in point 13 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council;
- 10) 'ICT product' means an ICT product as defined in point 12 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council;
- 11) 'information security service provider' means a managed service provider that carries out or provides assistance for risk management;
- 12) 'internet exchange point' means a network facility which enables the interconnection of more than two independent networks and the exchange of internet traffic between them, and which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;
- 13) 'online marketplace' means an online marketplace for the purposes of the Consumer Protection Act;
- 14) 'ex post inspection' means supervision related to an ex post response to a cyber incident or to additional verification of an imminent threat of a cyber incident, based on evidence, indications or information which has drawn the attention of the supervisory authority to a cyber incident or an imminent threat thereof, publicly available information, or information received or created by the supervisory authority in the performance of another task;
- 15) 'central government public administration entity' means Eesti Pank, a judicial body, the State Electoral Office, the Chancellery of the Riigikogu, the State Audit Office, the Office of the President of the Republic, a governmental authority, a state agency governed by a governmental authority, and the Office of the Chancellor of Justice;
- 16) 'local government public administration entity' means a local authority, a rural municipality or city administrative agency, an agency under the administration of a rural municipality or city administrative agency, a rural municipality district, a city district, an administrative agency of a rural municipality district or city district, an agency under the administration of an administrative agency of a rural municipality district or city district, and a joint administrative agency and joint agency of local authorities;
- 17) 'qualified trust service provider' means a qualified trust service provider as defined in point 20 of Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.08.2014, pp 73–114);
- 18) 'cyber incident handling' means any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from a cyber incident;
- 19) 'cyber incident' means an event in a network and information system that poses a risk to or compromises the security of the network and information system;
- 20) 'cyber incident handling unit' means a group of experts whose task is to carry out operations supporting cyber incident handling;

- 21) ‘cyber threat’ means a cyber threat as defined in point 8 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council;
- 22) ‘cybersecurity’ means cybersecurity as defined in point 1 of Article 2 of Regulation (EU) 2019/881 of the European Parliament and of the Council;
- 23) ‘significant cyber threat’ means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the network and information system of an entity or the users of the entity’s network and information system by causing considerable material or non-material damage;
- 24) ‘cloud computing service’ means an information society service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;
- 25) ‘risk’ means the potential for loss or disruption caused by a cyber incident, expressed as a combination of the magnitude of the loss or disruption and the likelihood of occurrence of the cyber incident;
- 26) ‘targeted security audit’ means an independent review and examination of network and information system datasets and operations to verify the adequacy of the security measures of the network and information system and compliance with applicable information security policies and operating procedures, to detect security breaches, and to recommend possible consequential changes to measures, policies and procedures;
- 27) ‘content delivery network’ means a network of geographically distributed servers for the purpose of ensuring high availability, accessibility or fast delivery of digital content and information society services to internet users on behalf of content and service providers;
- 28) ‘social media platform’ means a platform that enables end-users to connect, share, discover and communicate with each other across multiple devices, in particular via chats, posts, videos and recommendations;
- 29) ‘research organisation’ means an entity whose principal activity is to carry out applied research or product development with a view to exploiting the results of such research or development for commercial purposes, but which is not an educational institution;
- 30) ‘top-level domain name registry’ means an entity which has been delegated the top-level domain associated with the Estonian country code and is responsible for administering that top-level domain, including the registration of domain names under that top-level domain and the technical operation of the top-level domain, including the operation of its name servers, the maintenance of its databases and the distribution of top-level domain zone files across name servers, irrespective of whether any of those operations are carried out by the entity itself or are outsourced, but excluding situations where the registry uses top-level domain names only for its own use;
- 31) ‘vulnerability’ means a weakness, susceptibility or flaw of an ICT product or ICT service that can be exploited by a cyber threat;
- 32) ‘security assessment’ means a technical and organisational investigation of a network and information system to identify a vulnerability of the network and information system or non-compliance of the security measures of the network and information system with applicable requirements;
- 33) ‘security measures’ means organisational, physical and information technology actions or means applied to achieve and maintain the security of data and network and information systems;
- 34) ‘large-scale cyber incident’ means a cyber incident which causes a level of disruption that exceeds a European Union Member State’s capacity to respond to it or which has a significant impact on at least two European Union Member States;
- 35) ‘trust service provider’ means a trust service provider as defined in point 19 of Article 3 of Regulation (EU) No 910/2014 of the European Parliament and of the Council;
- 36) ‘online search engine’ means an online search engine as defined in point 5 of Article 2 of Regulation (EU) 2019/1150 of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.07.2019, pp 57–79);
- 37) ‘network and information system’ (hereinafter *system*) means an electronic communications network for the purposes of clause 8 of § 2 of the Electronic Communications Act, a device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data, or digital data stored, processed, retrieved or transmitted by the aforesaid elements for the purposes of their operation, use, protection or maintenance;
- 38) ‘security of a network and information system’ (hereinafter *security of system*) means the ability of the system to resist any event that threatens the availability, authenticity, integrity and confidentiality of data processed in the system or of the services offered by, or accessible via, the system;
- 39) ‘entity’ means a legal person created and recognised under the law of the country of its place of establishment, which may have rights and obligations, or a natural person;
- 40) ‘publicly available electronic communications service’ means a publicly available electronic communications service for the purposes of the Electronic Communications Act;
- 41) ‘public electronic communications network’ means a public electronic communications network for the purposes of the Electronic Communications Act.
- [RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 3. Service provider

- (1) For the purposes of this Act, ‘service provider’ means an entity essential for the functioning of society (hereinafter *essential entity*) and an entity important for the functioning of society (hereinafter *important entity*).

(2) An essential entity is:

- 1) a domain name system service provider;
- 2) a provider of a vital service for the purposes of the Emergency Act;
- 3) a central government public administration entity;
- 4) a local government public administration entity;
- 5) a provider of critical communications services, marine radio communications services and operational communications network services;
- 6) a qualified trust service provider;
- 7) a top-level domain name registry;
- 8) a provider of a public electronic communications network service or a provider of a publicly available electronic communications service who, according to the definition of a medium-sized enterprise set out in Commission Recommendation 2003/361/EC on the definition of micro, small and medium-sized enterprises (OJ L 124, 20.05.2003, pp 36–41), employs 50 or more persons during a financial year and whose annual balance sheet total or annual turnover exceeds 10 million euros.

(3) In addition to that provided in subsection 2 of this section, an essential entity also includes an entity which, according to the definition of a medium-sized enterprise set out in Commission Recommendation 2003/361/EC, employs 250 or more persons during a financial year and whose annual balance sheet total exceeds 43 million euros or whose annual turnover exceeds 50 million euros, and which is:

- 1) a data centre service provider;
- 2) an electricity undertaking for the purposes of the Electricity Market Act which engages in the sale of electricity, including the resale thereof to an electricity wholesaler or an end customer;
- 3) an electricity undertaking for the purposes of the Electricity Market Act which engages in the generation of electricity;
- 4) an undertaking engaged in the collection, discharge or treatment of urban waste water, domestic waste water or industrial waste water as defined in points 1, 2 and 3 of Article 2 of Council Directive 91/271/EEC concerning urban waste-water treatment (OJ L 135, 30.05.1991, pp 40–52), except for an undertaking for which the collection, discharge or treatment of urban waste water, domestic waste water or industrial waste water constitutes an insignificant part of its overall activities;
- 5) an undertaking indicated, as regards maritime transport, in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council on enhancing ship and port facility security (OJ L 129, 29.04.2004, pp 6–91), which engages in the carriage of passengers and freight on inland waterways, at sea and in coastal waters, except for individual vessels operated by that undertaking;
- 6) a manufacturer of a critical medical device in a public health emergency specified in Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices (OJ L 20, 31.01.2022, pp 1–37);
- 7) a manufacturer of basic pharmaceutical products and pharmaceutical preparations referred to in Division 21 of Section C of NACE Revision 2, the statistical classification of economic activities in the European Community;
- 8) a gas undertaking for the purposes of the Natural Gas Act;
- 9) a managed service provider;
- 10) a storage network operator for the purposes of the Natural Gas Act;
- 11) an information security service provider;
- 12) an internet exchange point service provider;
- 13) a distribution network operator for the purposes of the Electricity Market Act;
- 14) an operator of a district heating and district cooling system for the purposes of the District Heating Act;
- 15) a trading venue operator for the purposes of the Securities Market Act;
- 16) a central counterparty for the purposes of point 1 of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.07.2012, pp 1–59);
- 17) an operator of ground-based infrastructure, owned, managed or operated by the Republic of Estonia or by a person governed by private law, which supports the provision of space-based services and which is not a provider of a public electronic communications network service;
- 18) a credit institution for the purposes of point 1 of Article 4 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);
- 19) an operator of a recharging point for the purposes of the Electricity Market Act, who is responsible for managing and operating the recharging point by providing a recharging service to end users, including on behalf of, and for, a mobility service provider;
- 20) an air carrier for the purposes of point 4 of Article 3 of Regulation (EC) No 300/2008 of the European Parliament and of the Council on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 09.04.2008, pp 72–84), which engages in commercial air transport;
- 21) a managing body of an airport as defined in point 1 of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council on airport charges (OJ L 70, 14.03.2009, pp 11–16), and an operator of airport ancillary installations;
- 22) an airport operator for the purposes of the Aviation Act;
- 23) an air traffic management undertaking providing air traffic control services for the purposes of point 6 of Article 2 of Regulation (EU) 2024/2803 of the European Parliament and of the Council on the implementation of the Single European Sky (recast) (OJ L, 2024/2803, 11.11.2024);
- 24) an operator of an intelligent transport system for the purposes of the Traffic Act;
- 25) an operator of a natural gas refining and processing facility;

- 26) a gas undertaking for the purposes of the Natural Gas Act which engages in the sale of natural gas, including liquefied natural gas, and in the resale of natural gas to a wholesaler, an end customer and a gas undertaking purchasing natural gas;
- 27) a nominated electricity market operator for the purposes of point 8 of Article 2 of Regulation (EU) 2019/943 of the European Parliament and of the Council on the internal market for electricity (recast) (OJ L 158, 14.06.2019, pp 54–124);
- 28) an undertaking engaged in operating oil production, refining and processing facilities and in oil storage and transfer;
- 29) a cloud computing service provider;
- 30) a transmission network operator for the purposes of the Electricity Market Act;
- 31) a railway infrastructure undertaking and a railway undertaking, including an operator of a service facility, for the purposes of the Railways Act;
- 32) a port operator or a holder of a port facility for the purposes of the Ports Act, including a holder of a port facility as defined in point 11 of Article 2 of Regulation (EC) No 725/2004 of the European Parliament and of the Council, and an entity engaged in managing operations and equipment in ports;
- 33) a content delivery network service provider;
- 34) a market participant for the purposes of point 25 of Article 2 of Regulation (EU) 2019/943 of the European Union and of the Council who provides an aggregation service, a demand response service or an electricity storage service for the purposes of the Electricity Market Act;
- 35) an LNG terminal operator for the purposes of the Natural Gas Act;
- 36) a vessel traffic management centre;
- 37) a drinking water supplier and its distributor according to subsection 1 of § 17 of the Water Act, except for a distributor for which the distribution of drinking water constitutes an insignificant part of its overall activity of supplying other consumer goods and goods;
- 38) an undertaking engaged in hydrogen production, storage and transmission;
- 39) an entity engaged in the research and development of a medicinal product for the purposes of the Medicinal Products Act, except for a veterinary medicinal product as defined in point 1 of Article 4 of Regulation (EU) 2019/6 of the European Parliament and of the Council on veterinary medicinal products and repealing Directive 2001/82/EC (OJ L 4, 07.01.2019, pp 43–167);
- 40) an entity which engages in the formation and management of a liquid fuel reserve for the purposes of the Liquid Fuel Reserve Act;
- 41) an entity which performs the task of distributing natural gas and is responsible for the operation of the distribution system by ensuring the maintenance of that distribution system and, where necessary, the development thereof in a given area, and which, where necessary, ensures the interconnection of the natural gas network with other natural gas networks and the long-term ability of the natural gas network to meet reasonable demand for the distribution of natural gas;
- 42) an entity which performs the task of transmitting natural gas and is responsible for the operation of the transmission system by ensuring the maintenance of that transmission system and, where necessary, the development thereof in a given area, and which, where necessary, ensures the interconnection of the natural gas network with other natural gas networks and the long-term ability of the natural gas network to meet reasonable demand for the transmission of natural gas.

(4) An important entity is:

- 1) the controller and the processor of a database for the purposes of the Public Information Act;
- 2) the Foresight Centre;
- 3) a legal person governed by public law;
- 4) an association of local authorities;
- 5) a provider of family physician care for the purposes of the Health Services Organisation Act who is not a provider of a vital service;
- 6) the State Forest Management Centre;
- 7) a trust service provider, except for a qualified trust service provider;
- 8) an entity which is not an essential entity, but which, according to the definition of a medium-sized enterprise set out in Commission Recommendation 2003/361/EC, employs 50 or more persons during a financial year and whose annual balance sheet total or annual turnover exceeds 10 million euros and whose sector is listed in subsection 3 of this section;
- 9) a provider of a publicly available electronic communications service and a provider of a public electronic communications network service who does not meet the conditions specified in clause 8 of subsection 2 of § 3 of this Act.

(5) In addition to that specified in subsection 4 of this section, an important entity also includes an entity which, according to the definition of a medium-sized enterprise set out in Commission Recommendation 2003/361/EC, employs 50 or more persons during a financial year and whose annual balance sheet total or annual turnover exceeds 10 million euros, and which is:

- 1) an undertaking whose principal activity is waste management for the purposes of the Waste Act, including supervision over waste handling and aftercare of a waste management facility intended for the disposal of waste;
- 2) an undertaking which manufactures substances for the purposes of point 9 of Article 3 of Regulation (EC) No 1907/2006 of the European Parliament and of the Council concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) and establishing a European Chemicals Agency,

amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93, Commission Regulation (EC) No 1488/94, Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 396, 30.12.2006, pp 1–850), and places substances or mixtures on the market for the purposes of Article 3(14) of that Regulation, and an undertaking which manufactures articles as defined in point 3 of Article 3 of that Regulation from substances or mixtures;

3) an undertaking engaged in the wholesale, industrial manufacture or industrial processing of food, or in more than one of those activities, except for the wholesale, industrial manufacture and industrial processing of alcohol, in an undertaking as defined in point 2 of Article 3 of Regulation (EC) No 178/2002 of the European Parliament and of the Council laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31, 01.02.2002, pp 1–24), and the annual turnover derived from one or more of those activities constitutes at least 50 per cent of its annual turnover;

4) a manufacturer of a medical device as defined in point 1 of Article 2 of Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (OJ L 117, 05.05.2017, pp 1–175), and a manufacturer of an in vitro diagnostic medical device as defined in point 2 of Article 2 of Regulation (EU) 2017/746 of the European Parliament and of the Council on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (OJ L 117, 05.05.2017, pp 176–332), except for a manufacturer of a medical device referred to in clause 6 of subsection 3 of this section;

5) an undertaking engaged in economic activities referred to in Divisions 26–30 of Section C of NACE Revision 2, the statistical classification of economic activities in the European Community;

6) a provider of an online marketplace;

7) a postal service provider for the purposes of the Postal Act, including a courier service provider;

8) a provider of a social media platform;

9) a research organisation;

10) a provider of an online search engine.

(6) For the purposes of this Act, Article 3(4) of the Annex to Commission Recommendation 2003/361/EC does not apply when determining the number of employees of an entity, its annual balance sheet total and its annual turnover.

(7) For the purposes of this Act, the data of partner enterprises or linked enterprises for the purposes of Commission Recommendation 2003/361/EC is not taken into account when determining the number of employees of an entity, its annual balance sheet total and its annual turnover, if, in respect of the systems used to provide services, the entity is independent of its partner enterprise or linked enterprise.

(8) A detailed list of the processing domains and food groups specified in clause 3 of subsection 5 of this section is established by a regulation of the minister in charge of the policy sector of food supply security. [RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 3¹. Notification obligation and list

(1) A service provider and a domain name registration service provider submit to the Estonian Information System Authority, for the compilation of the list specified in subsection 2 of this section, at least the following information:

1) name and registry code;

2) the address of the place of business and up-to-date contact details, including e-mail addresses, Internet Protocol address ranges and telephone numbers;

3) where appropriate, the relevant sector and subsector referred to in Annex I or II to Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, pp 80–152);

4) where appropriate, a list of the countries in which it provides services falling within the scope of Directive (EU) 2022/2555 of the European Parliament and of the Council.

(2) Every two years, the Estonian Information System Authority compiles a list of service providers and domain name registration service providers.

(3) The information specified in subsection 2 of this section is information intended for internal use for the purposes of the Public Information Act.

(4) The service provider and the domain name registration service provider notify the Estonian Information System Authority of any changes to the information submitted pursuant to subsection 1 of this section without delay, but no later than two weeks after the date on which the change was made.

(5) Every two years, the Estonian Information System Authority informs the European Commission and the Cooperation Group specified in Article 14 of Directive (EU) 2022/2555 of the European Parliament and of the Council (hereinafter *Cooperation Group*) of the number of service providers entered in the list specified in subsection 2 of this section, for each sector and subsector referred to in Annex I or II to that Directive.

(6) Every two years, the Estonian Information System Authority submits to the European Commission information on entities which are essential entities and important entities on the basis of points b–e of Article 2(2) of Directive (EU) 2022/2555 of the European Parliament and of the Council.

(7) The information to be submitted on the basis of subsection 6 of this section is the number of entities, information on the sector and subsector referred to in Annexes I and II to Directive (EU) 2022/2555 of the European Parliament and of the Council and the type of services provided by the relevant service providers, together with information on which of points b–e of Article 2(2) of Directive (EU) 2022/2555 of the European Parliament and of the Council is the basis for considering an entity to be an essential entity or an important entity for the purposes of this Act.

(8) Upon request by the European Commission, the Estonian Information System Authority may forward to the Commission the names of the service providers referred to in subsection 6 of this section.

(9) In fulfilling the obligation provided in subsection 1 of this section, the service provider and the domain name registration service provider may follow the relevant European Commission guidelines and templates. [RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 4. Requirements related to digital service provider

(1) A digital service provider submits to the Estonian Information System Authority at least the following information:

- 1) name and registry code;
- 2) where relevant, information on the relevant sector, subsector and type of entity referred to in Annex I or II to Directive (EU) 2022/2555 of the European Parliament and of the Council;
- 3) the address of its main place of business and the addresses of its other official places of business in the European Union or, if it has no place of business in the European Union or is not established there, the address of the place of business of its representative;
- 4) its up-to-date contact details and, where relevant, the up-to-date contact details of its representative, including the e-mail address and telephone number;
- 5) the Member State or Member States where the service is provided;
- 6) Internet Protocol address ranges.

(2) Estonia is deemed to be the main place of business of a digital service provider if decisions concerning the security measures of that digital service provider are predominantly taken in Estonia.

(3) If it is not possible to determine the main place of business of a digital service provider pursuant to subsection 2 of this section or if such decisions are not taken in the European Union, Estonia is deemed to be the main place of business of the digital service provider concerned if the activities related to ensuring the cybersecurity of that digital service provider take place in Estonia.

(4) If it is not possible to determine the main place of business of a digital service provider pursuant to subsections 2 and 3 of this section, Estonia is deemed to be the main place of business of the digital service provider if the digital service provider has its place of business with the largest number of employees in the European Union within the territory of Estonia.

(5) Regardless of subsections 2–4 of this section, this Act applies to a digital service provider if the place of business of its representative is in Estonia or if its representative is established in Estonia.

(6) A digital service provider notifies of all changes to the information submitted pursuant to subsection 1 of this section without delay, but no later than three months after the date on which the change was made.

(7) The Estonian Information System Authority submits the information referred to in clauses 1–5 of subsection 1 of this section to the European Union Agency for Cybersecurity without undue delay.

(8) The Estonian Information System Authority may submit to the European Union Agency for Cybersecurity a request for access to the register specified in Article 27(1) of Directive (EU) 2022/2555 of the European Parliament and of the Council.

(9) In fulfilling the obligation provided in subsection 1 of this section, a digital service provider may follow the relevant European Commission guidelines and templates.

(10) A digital service provider providing services in Estonia but established outside the European Union must designate a representative in Estonia or in another Member State of the European Union where it provides the service or where it is established, and must make the contact details of the representative permanently publicly available.

(11) The designation of a representative of a digital service provider does not restrict the taking of legal measures in respect of the digital service provider.

(12) This Act also applies to a digital service provider that breaches the obligation to designate a representative in a Member State of the European Union.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 4¹. Initial compliance with requirements and obligations

(1) A service provider and a domain name registration service provider are to fulfil the obligation provided in subsection 1 of § 3¹ of this Act within three months as of the date on which they become compliant with the characteristics of a service provider or a domain name registration service provider.

(2) A digital service provider is to fulfil the obligations provided in subsections 1 and 10 of § 4 of this Act within three months as of the date on which it becomes compliant with the characteristics of a digital service provider.

(3) A service provider, including a digital service provider, is to bring its activities into conformity with the requirements of this Act and the requirements established on the basis thereof and is to fulfil the obligations arising from this Act and legislation established on the basis thereof within three years as of the date on which it becomes compliant with the characteristics of a service provider, including a digital service provider. The service provider is to fulfil the obligation provided in subsections 1 and 2 of this section within the time limits specified in those subsections.

(4) Regardless of subsection 3 of this section, a provider of a vital service must bring its activities into conformity with the requirements of this Act and the requirements established on the basis thereof within the time limit determined in accordance with the rules provided in clause 3 of subsection 1³ of § 38 of the Emergency Act. A provider of a vital service is to fulfil the obligation provided in subsections 1 and 2 of this section within the time limits specified in those subsections.

(5) This section does not apply to service providers to whom § 28¹ of this Act applies.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 5. Competent authorities and tasks

(1) The Government of the Republic adopts the national cybersecurity strategy specified in Article 7 of Directive (EU) 2022/2555 of the European Parliament and of the Council, which may be prepared as part of a document provided by another legal instrument. The preparation of the national cybersecurity strategy is co-ordinated by the minister in charge of the policy sector of national cybersecurity.

(2) The scope of the national cybersecurity strategy, the conditions and the procedure for implementation thereof, together with a list of the relevant policy measures, are established by a regulation of the minister in charge of the policy sector of national cybersecurity.

(3) The Estonian Information System Authority performs the following tasks specified in Directive (EU) 2022/2555 of the European Parliament and of the Council:

- 1) the tasks of the competent authority specified in Article 8(1) and of the single point of contact specified in Article 8(3);
- 2) the tasks of the competent authority responsible for the management of large-scale cyber incidents and crises specified in Article 9(1);
- 3) the tasks of a computer security incident response team specified in Article 10(1);
- 4) the tasks of the co-ordinator for co-ordinated vulnerability disclosure specified in Article 12(1);
- 5) the tasks related to participation in the network of national computer security incident response teams specified in Article 15 (hereinafter *network*).

(4) A security authority performs the tasks of the competent authority specified in Article 8(1) of Directive (EU) 2022/2555 of the European Parliament and of the Council to the extent provided in § 14 of this Act.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 5¹. European Cybersecurity Industrial, Technology and Research Competence Centre and National Coordination Centre

(1) For the purposes of Article 12 of Regulation (EU) 2021/887 of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L, 202, 08.06.2021, pp 1–31), the representative and alternate of the Governing Board of the European Cybersecurity Industrial, Technology and Research Competence Centre are appointed by a directive of the minister in charge of the policy sector.

(2) For the purposes of Article 6 of Regulation (EU) 2021/887 of the European Parliament and of the Council, the functions of the national coordination centre are performed by the Estonian Cybersecurity Industrial, Technology and Research Coordination Centre.

(3) The coordination centre specified in subsection 2 of this section is appointed and the procedure for the performance of its functions is established by a regulation of the minister in charge of the policy sector.
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

§ 5². Competent authority carrying out cybersecurity supervision in field of cross-border electricity flows

(1) The competent authority specified in Article 4(1) of Commission Delegated Regulation (EU) 2024/1366 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (OJ L, 2024/1366, 24.05.2024) is designated by a directive of the minister in charge of the policy sector of national cybersecurity.

(2) When designating the competent authority specified in subsection 1 of this section, the requirements provided in Article 4(3) of Commission Delegated Regulation (EU) 2024/1366 and in the Administrative Co-operation Act are taken into account.

(3) The Government of the Republic may further delegate the performance of the tasks referred to in Article 39(1), Article 40(4) and Article 41(1) and (2) of Commission Delegated Regulation (EU) 2024/1366 to the regional co-ordination centre established pursuant to Article 35 of Regulation (EU) 2019/943 of the European Parliament and of the Council on the internal market for electricity (OJ L 158, 14.06.2019, pp 54–124), taking into account the requirements provided in the Administrative Co-operation Act.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 6. Principles of ensuring cybersecurity

The following principles are taken into account in ensuring cybersecurity:

- 1) the principle of personality – ensuring the security of a system is arranged by the service provider;
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]
- 2) the principle of integral protection – the service provider ascertains potential risks posed to the system and applies appropriate organisational and technical measures for the protection of the system;
[RT I, 30.12.2025, 4 – entry into force 30.01.2026]
- 3) the principle of minimising adverse effect – in the case of a cyber incident the service provider applies due care and measures to avoid the escalation of the effect of the cyber incident and its possible spread to another system and notifies the supervisory authority provided in this Act of the cyber incident;
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]
- 4) the principle of co-operation – in ensuring cybersecurity and resolving cyber incidents the parties co-operate and, where necessary, take into account the mutual connection between and dependence of the systems and services.

Chapter 2 Obligations for Ensuring Cybersecurity

§ 6¹. Obligations of member of management board of service provider

(1) A service provider is to designate at least one member of the management board who approves the security measures, oversees their implementation and is responsible therefor. At the request of the Estonian Information System Authority, the service provider submits the name and contact details of the relevant member or members of the management board. The obligation to designate a responsible member of the management board does not apply to a service provider that has one member of the management board.

(2) The member of the management board of a service provider specified in subsection 1 of this section undergoes regular training with the aim of acquiring sufficient knowledge and skills to understand and assess risks, their impact on the services of the service provider and the ways of managing risks.

(3) If a service provider does not designate the member of the management board specified in subsection 1 of this section, the obligations provided in this section apply to all members of the management board.

(4) If a service provider, due to its legal form or structure, has no member of the management board, the provisions concerning a member of the management board also apply to another person who, under the law, the articles of association or another legal instrument, is designated in the service provider to perform management functions. If the service provider is a sole proprietor, the provisions concerning the obligations of a member of the management board of a service provider apply to the respective natural person.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 7. Security measures of service provider's system

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(1) A service provider implements, on a permanent basis, appropriate and proportionate technical, operational and organisational security measures in order to:

- 1) manage risks posed to the security of the system used in the activities of the service provider or in providing the service, including by preparing a corresponding risk assessment;
- 2) prevent or minimise the impact of a cyber incident on the recipient of the service provided by the service provider and on another service;
- 3) prevent a cyber incident or detect and respond to it.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(2) In implementing security measures, the following are taken into account:

- 1) the needs and security requirements of the service provider;
- 2) up-to-date and, where relevant, European and international standards;
- 3) the costs of implementing security measures;
- 4) the proportionality of implementing security measures, in the assessment of which, among other things, the degree of the service provider's exposure to risks, the size of the service provider, the likelihood and severity of cyber incidents, including the societal and economic impact of cyber incidents, are taken into account;
- 5) a systematic and comprehensive approach to threats with the aim of protecting systems and the physical environment of those systems against cyber incidents.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(3) If a service provider authorises another person to manage the system or hosts the system with another person, the service provider is responsible for making sure that the other person ensures the implementation of the security measures of the system.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(4) [Repealed – RT I, 06.08.2022, 2 – entry into force 16.08.2022]

(5) For ensuring the performance of the obligations provided in this section and the cybersecurity of systems, the Government of the Republic or a minister authorised thereby establishes by a regulation:

- 1) requirements for information security management under general title 'Estonian Information Security Standard';
- 2) general requirements for security measures;
- 3) special requirements for system security measures and the scope of application of such requirements.

[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

(6) The regulation established on the basis of subsection 5 of this section may specify the permanent appropriate and proportionate technical, operational and organisational security measures and the requirements and conditions for implementation thereof, including by taking into account the fields of activity specified in subsections 2–5 of § 3 of this Act.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(7) A service provider specified in an implementing act referred to in Article 21(5) of Directive (EU) 2022/2555 of the European Parliament and of the Council, laying down the technical and the methodological requirements, as well as sectoral requirements, as necessary, for the implementation of security measures by the service provider, follows, for the service specified in that implementing act, the requirements established by the same implementing act.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 8. Obligation of service provider to notify of cyber incident

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(1) A service provider, except for a security authority, submits to the Estonian Information System Authority an initial notification without delay, but no later than 24 hours after becoming aware of a cyber incident:

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

- 1) which has a significant impact on the security of the system or the continuity of the service;
- 2) a significant impact of which on the security of the system or the continuity of the service is not obvious but can be reasonably presumed.

(1¹) If a service provider authorises another person to manage the system or hosts the system with another person, the service provider is responsible for ensuring that the other person notifies the service provider no later than 24 hours after becoming aware of a cyber incident specified in subsection 1 of this section.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(2) A cyber incident has a significant impact if at least one of the following conditions is met:

- 1) the impact of the cyber incident is at least severe according to the severity of consequences determined in the system risk assessment prepared on the basis of clause 1 of subsection 1 of § 7 of this Act;

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

2) due to the cyber incident the provision of the service cannot be continued after the passing of the maximum permitted time of disruption of the service provided by the relevant service level agreement or the requirements for the continuity of the service;

3) the continuity of the service of the provider of another service is disrupted due to the cyber incident;
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

4) the extraordinary measures set out in the system risk assessment prepared under clause 1 of subsection 1 of § 7 of this Act or in another document, if any, describing the restoration of the continuity of the service or the security of the system need to be applied for responding to the cyber incident;

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

5) the service provider, another service provider or the service users suffer or may suffer significant damage due to the cyber incident;

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

6) it is a significant incident provided in a European Commission implementing act adopted under Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(3) If as a result of a cyber incident the provision of the service or another service is disrupted in at least one more European Union Member State, the cyber incident is always deemed to be of significant impact.

(4) [Repealed – RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(4¹) A service provider, except for a security authority, forwards to the Estonian Information System Authority without delay, but no later than 72 hours after becoming aware of a cyber incident with a significant impact, an incident notification updating the information submitted in the initial notification in order to obtain a specified overview of the circumstances of the cyber incident with a significant impact.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(4²) A trust service provider submits the incident notification specified in subsection 4¹ of this section without delay, but no later than 24 hours after becoming aware of a cyber incident with a significant impact.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(4³) At the request of the Estonian Information System Authority, a service provider submits, before submitting the final report specified in subsection 7 of this section, an interim report on the status of responding to the cyber incident with a significant impact. The interim report is to contain the data prescribed in the incident notification and, where relevant, additional information requested by the Estonian Information System Authority.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(5) Where relevant, a service provider is required to inform, within a reasonable time, a person who may be affected by a cyber incident with a significant impact or by a significant cyber threat, or the public if the affected persons cannot be informed individually. In the notification, the service provider, where possible, provides information about the significant cyber threat and the measures which the affected person may take in order to respond to the significant cyber threat.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(6) Where public awareness or the disclosure of a cyber incident is necessary to prevent or deal with a cyber incident with a significant impact or otherwise in the public interest, the Estonian Information System Authority may, after consulting the relevant service provider, inform the public of the cyber incident with a significant impact or require the relevant service provider to do so.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(7) A service provider submits a final report to the Estonian Information System Authority within one month as of the submission of the incident notification specified in subsection 4¹ of this section. If the cyber incident with a significant impact has not yet been resolved by the time the final report is submitted, the submitted final report is treated as an interim report and the service provider submits a new final report within one month after the cyber incident with a significant impact has been resolved.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(8) The data to be submitted when notifying of a cyber incident and the procedure for notification are established by a regulation of the minister in charge of the policy sector of national cybersecurity.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(8¹) If the European Commission adopts an implementing act specified in Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council, specifying the format of, and the procedure for submitting, a notification or report on a cyber incident, including a cyber incident with a significant impact, the requirements provided in that implementing act must be followed.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(9) [Repealed – RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(10) A security authority notifies a cyber incident to the relevant security authority, taking into account the requirements provided in this section.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 8¹. Voluntary notification

(1) The Estonian Information System Authority may be:

1) notified of a cyber incident, a vulnerability and a cyber threat by a service provider;
2) notified of a cyber incident with a significant impact, a vulnerability and a cyber threat by a person other than a service provider.

(2) A natural or legal person notifying of a potential vulnerability or a vulnerability may submit a notification anonymously. The personal data of the person submitting the notification is information intended for internal use for the purposes of the Public Information Act.

(3) The Estonian Information System Authority processes notifications submitted on the basis of subsection 1 of this section in accordance with the rules provided in §§ 8 and 12 of this Act.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 9. Security measures of state and local authority's system

[Repealed – RT I, 06.08.2022, 2 – entry into force 16.08.2022]

§ 10. Security measures of digital service provider's system

[Repealed – RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 11. Obligation of digital service provider to notify of cyber incident

[Repealed – RT I, 30.12.2025, 4 – entry into force 01.01.2026]

Chapter 3 Ensuring Cybersecurity

§ 12. Prevention of and response to cyber incident

(1) Ensuring cybersecurity and preventing and responding to a cyber incident to the extent provided by this Act is co-ordinated by the Estonian Information System Authority.

(2) For the purpose of ensuring cybersecurity, the Estonian Information System Authority observes domains in the Estonian Internet protocol address space and related to the Estonian country code, analyses risks posed to the security of systems and the impact thereof on the state, society and the security of systems.

(3) For the purpose of preventing and responding to a cyber incident, the Estonian Information System Authority sends people alerts enabling them to take measures avoiding or reducing the impact of the cyber incident.

(3¹) The Estonian Information System Authority provides to the entity that has notified it of a cyber incident with a significant impact a response, where possible, within 24 hours, which contains preliminary feedback on the cyber incident with a significant impact and, upon request of the entity submitting the notification, also guidance on measures for responding to the cyber incident with a significant impact.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(3²) In responding to a cyber incident, the Estonian Information System Authority may give priority to the processing of a notification submitted on the basis of § 8 of this Act over the processing of a notification submitted on the basis of § 8¹.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(4) The Estonian Information System Authority has the right to forward to a foreign state or to the European Union Agency for Cybersecurity or to another organisation information related to the prevention of and response to a cyber incident for the performance of the tasks provided in § 5 of this Act or of an obligation arising from European Union law, or in the cases and in accordance with the rules provided in an international agreement, provided the forwarded information does not prejudice national security or criminal proceedings. The forwarding of such information is mandatory in particular where a cyber incident with a significant impact concerns two or more Member States of the European Union, in which case the relevant information concerning the cyber incident with a significant impact must be forwarded to the affected foreign state and to the European Union Agency for Cybersecurity.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(4¹) Every three months, the Estonian Information System Authority submits to the European Union Agency for Cybersecurity a consolidated report containing anonymous aggregate data on cyber threats, cyber incidents and cyber incidents with a significant impact.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(5) The Estonian Information System Authority forwards the information specified in subsections 4 and 41 of this section only to the extent necessary and proportionate for the purpose of information sharing, protecting the security and commercial interests of the service provider and abiding by the obligation to maintain business secrecy.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 12¹. Prevention of and response to large-scale cyber incident and crisis

(1) The provisions of § 12 of this Act and of other sector-specific Acts governing the prevention of and response to crises apply to the prevention of and response to a large-scale cyber incident and crisis.

(2) The Estonian Information System Authority:

1) draws up and adopts a large-scale cyber incident and crisis response plan (hereinafter *plan*), taking into account the requirements provided in Article 9(4) of Directive (EU) 2022/2555 of the European Parliament and of the Council;

2) notifies the European Commission within three months of the adoption of the plan or of amendments to the adopted plan and submits to the European Commission and to the European cyber crisis liaison organisation network, within three months after the adoption of the plan, relevant information related to the plan.

(3) The plan may be drawn up as part of a document drawn up under another legal instrument.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 13. Cyber incident registry

(1) The cyber incident registry (hereinafter *registry*) is a database maintained by the Estonian Information System Authority, where data describing the occurrence of a cyber incident, cyber threats and vulnerabilities is entered for the purpose of keeping record of cyber incidents, cyber threats and vulnerabilities and analysing the information submitted to the registry for the prevention of or response to cyber incidents, cyber threats and vulnerabilities, for forwarding alerts and for performing supervisory operations.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(1¹) The name and contact details of the notifier of a cyber incident, cyber threat or vulnerability (hereinafter collectively *data provider*) are entered in the registry.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(2) Access to the registry is restricted and the registry data is intended for internal use, unless otherwise provided by legislation.

(3) The statutes of the registry are established by a regulation of the minister in charge of the policy sector.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(4) The regulation specified in subsection 3 of this section provides for:

1) the detailed composition of the data;

2) the data providers;

3) the procedure for ensuring the accuracy of the data;

4) the conditions for access to the data;

5) the detailed conditions for registry operations and for the retention of data entered in the registry;

6) the financing of the registry;

7) other organisational requirements related to the registry.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(5) Data entered in the registry or related to the registry is retained as follows:

1) data on cyber incidents entered in the registry is retained for five years as of the response to the cyber incident;

2) other data entered in the registry is retained for five years as of entry in the registry;

3) data on registry operations is retained for three years.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

Chapter 3¹

Cybersecurity Certification

[RT I, 06.08.2022, 2 - entry into force 16.08.2022]

§ 13¹. National cybersecurity certification authority

The national cybersecurity certification authority for the purposes of Article 58(1) of Regulation (EU) 2019/881 of the European Parliament and of the Council is the Consumer Protection and Technical Regulatory Authority.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 13². Cybersecurity conformity assessment body

Operating as a conformity assessment body and issuing an activity licence to a conformity assessment body are subject to §§ 22–31 and 33 and subsection 1 of § 35 of the Product Conformity Act, taking into account the specifications set out in Articles 60 and 61 and in an implementing act of the European Commission adopted under Article 61 of Regulation (EU) 2019/881 of the European Parliament and of the Council.
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

Chapter 4 State and Administrative Supervision

§ 14. Exercise of state and administrative supervision

(1) State and administrative supervision over compliance with the requirements provided in this Act and in legislation established on the basis of this Act is exercised by the Estonian Information System Authority.

(2) [Repealed – RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(3) [Repealed – RT I, 06.08.2022, 2 – entry into force 16.08.2022]

(4) The Consumer Protection and Technical Regulatory Authority exercises state and administrative supervision to the extent provided in Article 58(7) of Regulation (EU) 2019/881 of the European Parliament and of the Council.
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

(5) Administrative supervision over compliance with requirements for systems of a security authority as provided by this Act and legislation established on the basis of this Act is exercised by the relevant security authority. The provisions of subsections 1¹–3 of § 17 of this Act apply to the security authority exercising administrative supervision.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(6) The Estonian Information System Authority:
1) may, in exercising supervision, prioritise the performance of the tasks provided in this Act, taking into account a risk- or threat-prognosis-based approach;
2) exercises state and administrative supervision in respect of an essential entity;
3) exercises state and administrative supervision in respect of an important entity by way of ex post inspection where the supervisory authority has reason to believe that the important entity does not comply with the requirements provided in this Act and, in particular, in §§ 7 and 8 of this Act.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(7) In applying a state or administrative supervision measure, the circumstances of each individual case are taken into account, in particular:

- 1) the seriousness of the infringement and the importance of the requirements breached;
 - 2) the duration of the infringement;
 - 3) previous relevant infringements by the service provider concerned;
 - 4) the material or non-material damage caused, including the effects of financial or economic loss on other services;
 - 5) the number of persons affected by the infringement;
 - 6) the intent or negligence on the part of the perpetrator of the infringement;
 - 7) the security measures taken by the service provider to prevent or mitigate material or non-material damage;
 - 8) the status of adherence to approved codes of conduct or of implementation of approved certification mechanisms;
 - 9) co-operation between the supervisory authority specified in subsections 1 and 5 of this section and the service provider.
- [RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(8) For the purposes of clause 1 of subsection 7 of this section, the following infringements are deemed serious infringements:

- 1) repeated violations;

- 2) a failure by a service provider to fulfil the obligation provided in subsection 1 of § 8 of this Act;
- 3) in the event of a cyber incident with a significant impact, failure by the service provider to apply security measures to respond to the incident;
- 4) a failure to remedy the deficiencies indicated in a compliance notice of the supervisory authority specified in subsections 1 and 5 of this section;
- 5) the obstruction of audits or state supervision or administrative supervision ordered by the competent authority specified in subsections 1 and 5 of this section following the finding of an infringement;
- 6) providing false or grossly inaccurate information in relation to the implementation of the security measures provided in § 7 of this Act and the notification of a cyber incident with a significant impact provided in § 8 of this Act.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 15. Special state supervision measures

(1) In order to exercise the state supervision provided by this Act, law enforcement agencies may apply the special state supervision measures provided in §§ 30, 31, 32, 49, 50 and 51 of the Law Enforcement Act on the grounds and in accordance with the rules provided in the Law Enforcement Act.

(2) In exercising state supervision over compliance with the requirements provided in §§ 7 and 8 of this Act and legislation established on the basis thereof, or in an implementing act adopted on the basis of Article 21(5) or Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council, a law enforcement agency may, in addition to the special measures specified in subsection 1 of this section, also apply the special state supervision measure provided in § 52 of the Law Enforcement Act on the grounds and in accordance with the rules provided in the Law Enforcement Act.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 16. Specifications of state supervision

(1) For countering an immediate serious threat or eliminating a disturbance in case of a cyber incident the Estonian Information System Authority may restrict the use of or access to a system provided all the following conditions are met:

- 1) the cyber incident compromises or harms the security of another system;
- 2) the system administrator is unable or is unable in a timely manner to counter the serious threat or eliminate the disturbance originating from the cyber incident;
- 3) it is not possible to counter the serious threat or eliminate the disturbance originating from the cyber incident by using a less infringing measure;
- 4) a person is not caused disproportional damage by countering the serious threat or eliminating the disturbance originating from the cyber incident.

(1¹) In performing the tasks of state supervision, the Estonian Information System Authority has the right to:

- 1) carry out on-site inspections and off-site supervision in respect of a service provider, proceeding from clauses 2 and 3 of subsection 6 of § 14 of this Act, including to carry out random supervision in respect of an essential entity, which may, among other things, be prompted by a cyber incident with a significant impact or by a breach of a requirement provided in this Act or in an implementing act adopted on the basis thereof or on the basis of Article 21(5) or Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council;
- 2) carry out targeted security audits in respect of a service provider, based on a risk assessment performed by the Estonian Information System Authority or by the audited service provider, or on other available risk information, the costs of which are covered by the service provider, except in the cases specified in the regulation established on the basis of subsection 1² of this section;
- 3) carry out security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the co-operation of the service provider concerned;
- 4) issue a warning to a service provider where the service provider breaches this Act, or a requirement provided in an implementing act adopted on the basis of this Act or on the basis of Article 21(5) or Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council;
- 5) issue a compliance notice requiring the addressee of the compliance notice to cease an activity or practice which breaches a requirement provided in this Act, or in an implementing act adopted on the basis thereof or on the basis of Article 21(5) or Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council, and to refrain from using the same activity or practice;
- 6) issue a compliance notice requiring the addressee of the compliance notice to comply with the requirements provided in § 7 of this Act and in an implementing act adopted on the basis of this Act or on the basis of Article 21(5) of Directive (EU) 2022/2555 of the European Parliament and of the Council, and to submit a notification provided in § 8 of this Act in the manner referred to in that section and within the time limit specified;
- 7) issue a compliance notice requiring the addressee of the compliance notice to notify an entity where the service or activity provided to that entity by the addressee of the compliance notice may be affected by a significant cyber threat, by providing in the notification information on the significant cyber threat and, where possible, explanations as to which measures the affected entity may take to respond to the cyber threat;

8) issue a compliance notice requiring the addressee of the compliance notice to implement recommendations made on the basis of a security audit within a reasonable time;

9) issue a compliance notice requiring the addressee of the compliance notice to disclose the circumstances of a breach of a requirement provided in this Act or in an implementing act adopted on the basis of this Act or on the basis of Article 21(5) or Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council, in the manner prescribed in the compliance notice;

10) issue to an essential entity a compliance notice requiring the addressee of the compliance notice to designate, for a specified period, a compliance officer who monitors whether the addressee of the compliance notice complies with the requirements provided in §§ 7 and 8 of this Act and the requirements provided in an implementing act adopted on the basis thereof or on the basis of Article 21(5) or Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(1²) The detailed conditions and procedure for organising the targeted security audit specified in clause 2 of subsection 1¹ of this section, including a list of situations in which the Estonian Information System Authority reimburses the service provider the costs of the security audit, and the procedure for reimbursing the costs of the security audit are established by a regulation of the minister in charge of the policy sector of national cybersecurity.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(1³) The compliance notice issued to an essential entity specified in clause 5 of subsection 1¹ of this section may also include security measures intended to prevent or remedy a cyber incident and requirements regarding the deadline for implementing the security measures and notifying of implementation.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(1⁴) If the supervisory measures specified in clauses 4–6 and 8 of subsection 1¹ of this section in respect of an essential entity are ineffective, the Estonian Information System Authority sets the essential entity a new deadline for remedying deficiencies or for complying with the requirements set by the Estonian Information System Authority.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(1⁵) If an essential entity does not remedy deficiencies or comply with the requirements of the Estonian Information System Authority by the deadline set on the basis of subsection 1⁴ of this section, the Estonian Information System Authority has the right to require by a compliance notice:

1) the authorisation body to temporarily suspend a certification or authorisation concerning part or all of the relevant services or activities provided by the essential entity, or, where it has the relevant competence, to perform said actions itself;

2) the essential entity to temporarily suspend the powers of a member of the management board.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(1⁶) The measures provided in clauses 1 and 2 of subsection 1⁵ of this section are applied until the essential entity concerned takes the necessary measures to remedy deficiencies or to comply with the requirements of the Estonian Information System Authority.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(1⁷) For the exercise of state supervision, the Consumer Protection and Technical Regulatory Authority may take measures provided in Article 58(8) of Regulation (EU) 2019/881 of the European Parliament and of the Council.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026 – the number of the section changed from 1.1 to 1.7]

(2) The addressee is to be notified of the application of a measure provided in this section at the first opportunity.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(3) It is required to record a measure provided in this section.

§ 17. Administrative supervision measures

(1) Upon exercising administrative supervision, the Estonian Information System Authority is authorised to access a system and restrict the use of or access to the system provided all the following conditions are met:

1) a cyber incident compromises or harms the security of another system;

2) the system administrator is unable or is unable in a timely manner to counter a threat originating from the cyber incident or eliminate the cyber incident;

3) it is not possible to counter the threat originating from the cyber incident or eliminate the cyber incident by using a less infringing measure in respect of a person;

4) a person is not caused disproportional damage by countering the threat originating from the cyber incident or by eliminating the cyber incident.

(1¹) In performing the tasks of administrative supervision, the Estonian Information System Authority has the right to:

- 1) carry out on-site inspections and off-site supervision in respect of a service provider, proceeding from clauses 2 and 3 of subsection 6 of § 14 of this Act, including to carry out random supervision in respect of an essential entity, which may, among other things, be prompted by a cyber incident with a significant impact or by a breach of a requirement provided in this Act or in an implementing act adopted on the basis thereof or on the basis of Article 21(5) or Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council;
 - 2) carry out targeted security audits in respect of a service provider, based on a risk assessment performed by the Estonian Information System Authority or by the audited service provider, or on other available risk information, the costs of which are covered by the service provider, except in the cases specified in the regulation established on the basis of subsection 1² of this section;
 - 3) carry out security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria, where necessary with the co-operation of the service provider concerned;
 - 4) issue a warning to a service provider where the service provider breaches this Act, or a requirement provided in an implementing act adopted on the basis of this Act or on the basis of Article 21(5) or Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council;
 - 5) issue a compliance notice requiring the addressee of the compliance notice to cease an activity or practice which breaches a requirement provided in this Act, or in an implementing act adopted on the basis thereof or on the basis of Article 21(5) or Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council, and to refrain from using the same activity or practice;
 - 6) issue a compliance notice requiring the addressee of the compliance notice to comply with the requirements provided in § 7 of this Act and in an implementing act adopted on the basis of this Act or on the basis of Article 21(5) of Directive (EU) 2022/2555 of the European Parliament and of the Council, and to submit a notification provided in § 8 of this Act in the manner referred to in that section and within the time limit specified;
 - 7) issue a compliance notice requiring the addressee of the compliance notice to notify an entity where the service or activity provided to that entity by the addressee of the compliance notice may be affected by a significant cyber threat, by providing in the notification information on the significant cyber threat and, where possible, explanations as to which measures the affected entity may take to respond to the cyber threat;
 - 8) issue a compliance notice requiring the addressee of the compliance notice to implement recommendations made on the basis of a security audit within a reasonable time;
 - 9) issue a compliance notice requiring the addressee of the compliance notice to disclose the circumstances of a breach of a requirement provided in this Act or in an implementing act adopted on the basis of this Act or on the basis of Article 21(5) or Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council, in the manner prescribed in the compliance notice;
 - 10) issue to an essential entity a compliance notice requiring the addressee of the compliance notice to designate, for a specified period, a compliance officer who monitors whether the addressee of the compliance notice complies with the requirements provided in §§ 7 and 8 of this Act and the requirements provided in an implementing act adopted on the basis thereof or on the basis of Article 21(5) or Article 23(11) of Directive (EU) 2022/2555 of the European Parliament and of the Council.
- [RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(1²) The detailed conditions and procedure for organising the targeted security audit specified in clause 2 of subsection 1¹ of this section, including a list of situations in which the Estonian Information System Authority reimburses the service provider the costs of the security audit, and the procedure for reimbursing the costs of the security audit are established by a regulation of the minister in charge of the policy sector of national cybersecurity.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(1³) The compliance notice issued to an essential entity specified in clause 5 of subsection 1¹ of this section may also include security measures intended to prevent or remedy a cyber incident and requirements regarding the deadline for implementing the security measures and notifying of implementation.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(2) The addressee must be notified of the application of a measure provided in this section at the first opportunity.

(3) It is required to record a measure provided in this section.

§ 17¹. Rate of non-compliance levy

Upon failure to comply with a compliance notice, the upper limit of non-compliance levy for each imposition thereof in accordance with the rules provided in the Substitutional Performance and Non-Compliance Levies Act is 70,000 euros.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 17². Term for review of complaint

(1) The Consumer Protection and Technical Regulatory Authority settles a complaint provided in Article 63 of Regulation (EU) 2019/881 of the European Parliament and of the Council no later than on the 90th day as of the receipt of the complaint.

(2) Should the settlement of a complaint specified in subsection 1 of this section require co-operation with the national cybersecurity certification authority of another state, the Consumer Protection and Technical Regulatory Authority has the right to extend the term for review of the complaint by a period of time necessary for hearing the opinion of said authority. The person who lodged the complaint is informed of the extension of the term for review of the complaint in writing.

[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

§ 17³. Mutual assistance

(1) Where an entity provides services in more than one Member State of the European Union, or provides services in one or more Member States of the European Union and its systems are located in one or more other Member States of the European Union, the Estonian Information System Authority and the competent authorities designated in another Member State of the European Union on the basis of Article 8 of Directive (EU) 2022/2555 of the European Parliament and of the Council co-operate with and assist each other as necessary.

(2) Upon a substantiated request from the supervisory authority of another Member State of the European Union, the Estonian Information System Authority provides the other supervisory authority with assistance proportionate to its own resources so that the supervisory or enforcement measures can be implemented in an effective, efficient and consistent manner. Mutual assistance may, in particular, cover information requests and supervisory measures, including requests to carry out on-site inspections or off-site supervision or targeted security audits.

(3) In the case specified in subsection 1 of this section, the Estonian Information System Authority may submit a request for assistance referred to in subsection 2 of this section to the competent authority designated in another Member State of the European Union on the basis of Article 8 of Directive (EU) 2022/2555 of the European Parliament and of the Council.

(4) The Estonian Information System Authority may refuse a request for assistance submitted by the competent authority designated in another Member State of the European Union on the basis of Article 8 of Directive (EU) 2022/2555 of the European Parliament and of the Council if:

- 1) the Estonian Information System Authority does not have the competence to provide the requested assistance;
- 2) the requested assistance is not proportionate to the tasks of the Estonian Information System Authority; or
- 3) the request concerns information or entails activities which, if disclosed or carried out, would be contrary to the essential interests of national security, public security or national defence.

(5) Before refusing a request for assistance, the Estonian Information System Authority consults other relevant competent authorities and, upon the request of one of the Member States of the European Union concerned, also the European Commission and the European Union Agency for Cybersecurity.

(6) Taking into account the supervisory measures specified in this Act, the Estonian Information System Authority may apply joint supervisory measures involving employees or officials of a competent authority designated on the basis of Article 8 of Directive (EU) 2022/2555 of the European Parliament and of the Council. The authorities agree among themselves on the procedure and operations for joint activities.

(7) If Estonia receives, in relation to a digital service provider, a request for mutual assistance, the Estonian Information System Authority may, within the scope of the request, take appropriate supervisory and enforcement measures in respect of the digital service provider specified in the request, where that digital service provider provides services or manages systems within the territory of the Republic of Estonia.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

Chapter 4¹

Co-operation, Information Sharing and Peer Review

[RT I, 30.12.2025, 4 - entry into force 01.01.2026]

§ 17⁴. Co-operation tasks of Estonian Information System Authority and security authority

(1) In performing their tasks, the Estonian Information System Authority and a security authority co-operate with the following authorities and communities:

- 1) national authorities pursuant to Regulation (EC) No 300/2008 of the European Parliament and of the Council;

- 2) supervisory authorities pursuant to Regulation (EU) No 910/2014 of the European Parliament and of the Council;
- 3) national authorities pursuant to Regulation (EU) 2018/1139 of the European Parliament and of the Council on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (OJ L 212, 22.08.2018, pp 1–122);
- 4) competent authorities pursuant to Regulation (EU) 2022/2554 of the European Parliament and of the Council;
- 5) personal data protection supervisory authorities;
- 6) a security authority;
- 7) competent authorities pursuant to other European Union legal acts;
- 8) the Consumer Protection and Technical Regulatory Authority;
- 9) sector-specific or cross-sector communities of service providers, including, where necessary, exchange information with them, taking into account the requirements provided in § 17⁵ of this Act;
- 10) law enforcement agencies for the purposes of the Personal Data Protection Act.

(2) The Estonian Information System Authority co-operates comprehensively with an authority organising a vital service or an authority designated by it on the basis of subsection 5 of § 37 of the Emergency Act, the Rescue Board and the Government Office, and shares with them information regarding the designation of a provider of a vital service and the risks, cyber threats, cyber incidents and cyber incidents with a significant impact notified by a provider of a vital service, as well as other relevant situations, other than risks, cyber threats and cyber incidents, affecting essential entities that are regarded as providers of a vital service, and the measures taken to respond to such risks, threats and incidents. In addition, the Estonian Information System Authority notifies said authority if, in the course of state or administrative supervision, the Estonian Information System Authority applies a supervisory measure in respect of a provider of a vital service. The same authority may, where relevant, request the Estonian Information System Authority to apply a supervisory measure provided for in state or administrative supervision proceedings in respect of a provider of a vital service.

(3) The Estonian Information System Authority notifies the Oversight Forum established pursuant to Article 32(1) of Regulation (EU) 2022/2554 of the European Parliament and of the Council if, in the course of state supervision, the Estonian Information System Authority applies a supervisory measure to ensure compliance, by a service provider falling within the scope of application of this Act and designated as a critical ICT third-party service provider pursuant to Article 31 of that Regulation, with the requirements established in this Act or on the basis of this Act.

(4) The Estonian Information System Authority and the authorities specified in clauses 2, 4, 6 and 8 of subsection 1 of this section share relevant information regularly, including information on relevant cyber incidents and cyber threats.

(5) As the competent authority designated on the basis of Article 8(1) of Directive (EU) 2022/2555 of the European Parliament and of the Council, the Estonian Information System Authority exercises a liaison function to ensure cross-border co-operation, in the field of cybersecurity, between Estonian authorities and the relevant competent authorities of other Member States of the European Union and, where relevant, also the European Commission and the European Union Agency for Cybersecurity.

(6) In sharing information, the security of the information transmitted is ensured and, where relevant, agreed information-sharing protocols are used, including the traffic light protocol.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 17⁵. Cybersecurity information-sharing arrangements

(1) Service providers and other persons may exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

- 1) aims to prevent, detect, respond to or recover from cyber incidents or to mitigate their impact; or
- 2) enhances cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.

(2) The information sharing specified in subsection 1 of this section takes place on the basis of a cybersecurity information-sharing arrangement (hereinafter *information-sharing arrangement*). There may be more than one information-sharing arrangement.

(3) An information-sharing arrangement may specify operational elements, including the use of dedicated information and communications technology platforms and automation tools, and other content and conditions, taking into account the confidentiality of the information shared.

(4) The Estonian Information System Authority may impose conditions on the information made available by it under an information-sharing arrangement if a central government public administration entity or a local government public administration entity participates in the information-sharing arrangement.

(5) A service provider notifies the Estonian Information System Authority upon entering into an information-sharing arrangement or where withdrawal from an information-sharing arrangement has taken effect.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 17⁶. Peer review

(1) Participation in the peer review provided in Article 19 of Directive (EU) 2022/2555 of the European Parliament and of the Council (hereinafter *peer review*) is voluntary.

(2) In the course of the peer review, the participating cybersecurity experts are not to disclose to third parties information obtained in the course of the peer review, unless an equivalent obligation of confidentiality is provided by law.

(3) The minister in charge of the policy sector of national cybersecurity may establish by a regulation the detailed conditions and procedure for participation in the peer review, including requirements for the organisation of the peer review, the tasks of the authorities participating in it, and the persons participating in the peer review.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

Chapter 5 Liability

§ 18. Violation of requirements of Act

[Repealed – RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 18¹. Violation of requirements of Regulation (EU) 2019/881 of the European Parliament and of the Council

(1) Issue of a statement of conformity that does not comply with the conditions provided in Article 53(2) of Regulation (EU) 2019/881 of the European Parliament and of the Council or, in the event of information specified in Article 55(1), violation of the requirements provided in paragraph 2 of the same Article – is punishable by a fine of up to 200 fine units.

(2) The same act, if committed by a legal person, – is punishable by a fine of up to 20,000 euros.

[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

§ 18². Violation of requirements of Act by essential entity

(1) Violation, by an essential entity, of the requirements provided in subsection 1, 2, 3, 5 or 7 of § 7, or in subsection 1, 1¹, 4¹, 4², 4³, 5, 7 or 8¹ of § 8 of this Act, where the elements of a misdemeanour provided in § 18⁴ of this Act are absent, – is punishable by a fine of up to 10,000,000 euros.

(2) The same act, if committed by a legal person, – is punishable by a fine of up to 10,000,000 euros or up to 2 per cent of the total worldwide annual turnover of the essential entity in the preceding financial year, whichever amount is higher.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 18³. Violation of requirements of Act by important entity

(1) Violation, by an important entity, of the requirements provided in subsection 1, 2, 3, 5 or 7 of § 7, or in subsection 1, 1¹, 4¹, 4², 4³, 5, 7 or 8¹ of § 8 of this Act, where the elements of a misdemeanour provided in § 18⁴ of this Act are absent, – is punishable by a fine of up to 7,000,000 euros.

(2) The same act, if committed by a legal person, – is punishable by a fine of up to 7,000,000 euros or up to 1.4 per cent of the total worldwide annual turnover of the important entity in the preceding financial year, whichever amount is higher.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 18⁴. Violation of requirements of Act by entity in field of cross-border electricity flows

(1) Violation, by an entity specified in Article 2(1) of Commission Delegated Regulation (EU) 2024/1366, of the requirements provided in that Regulation, – is punishable by a fine of up to 10,000,000 euros.

(2) The same act, if committed by a legal person, – is punishable by a fine of up to 10,000,000 euros or up to 2 per cent of the total worldwide annual turnover of the entity in the preceding financial year, whichever amount is higher.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 18⁵. Violation of requirements of Act by legal representative of entity in field of cross-border electricity flows

(1) Violation, by a legal representative designated on the basis of Article 15(1) of Commission Delegated Regulation (EU) 2024/1366, of the requirements provided in that Regulation, – is punishable by a fine of up to 300 fine units.

(2) The same act, if committed by a legal person, – is punishable by a fine of up to 32,000 euros.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 19. Proceedings

(1) The body conducting extra-judicial proceedings pertaining to the misdemeanours provided in §§ 18²–18⁵ of this Act is the Estonian Information System Authority.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(2) If a misdemeanour provided in §§ 18²–18⁵ of this Act is related to a violation of the requirements for the processing of personal data, the Personal Data Protection Act is applied to the misdemeanour proceedings.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

(3) The body conducting extra-judicial proceedings pertaining to the misdemeanour provided in § 18¹ of this Act is the Consumer Protection and Technical Regulatory Authority.
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

(4) The limitation period for the misdemeanours provided in §§ 18²–18⁴ of this Act is three years.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

Chapter 6 Implementing Provisions

§ 20. Tasks of Estonian Information System Authority

(1) The Estonian Information System Authority compiles the list specified in subsection 2 of § 3¹ of this Act within six months as of the entry into force of that subsection.

(2) The Estonian Information System Authority forwards the information specified in subsections 5–7 of § 3¹ of this Act within six months as of the entry into force of those subsections.

(3) The Estonian Information System Authority forwards the first consolidated report pursuant to subsection 4¹ of § 12 of this Act within three months as of the entry into force of that subsection.
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 21.–§ 28.[Provisions governing the amendment of other Acts are omitted from this translation.]

§ 28¹. Bringing activities of service provider into conformity with this Act in connection with transposition of Directive (EU) 2022/2555 of European Parliament and of Council

(1) A service provider which, before the entry into force of subsection 1 of § 3¹ of this Act, met the characteristics of a service provider provided in this Act, is to fulfil the obligation provided in that subsection within three months as of the entry into force of that subsection.

(2) A digital service provider which, before the entry into force of subsection 7 of § 4 of this Act, met the characteristics of a service provider provided in this Act, is to fulfil the obligations provided in subsections 1 and 10 of § 4 of this Act within three months as of the entry into force of subsection 7 of § 4 of this Act.

(3) A service provider, including a digital service provider, which, before the entry into force of subsection 1 of § 3¹ of this Act, met the characteristics of a service provider provided in this Act, is to bring its activities into conformity with the requirements of this Act and the requirements established on the basis thereof within three years as of the entry into force of that subsection. The service provider is to fulfil the obligation provided in subsections 1 and 2 of this section within the time limits specified in those subsections.

(4) A provider of a vital service which became, for the first time, subject to the obligation to comply with this Act after 18 October 2024 and which, before the entry into force of subsection 1 of § 3¹ of this Act, met the characteristics of a service provider provided in this Act, is to bring its activities into conformity with the requirements of this Act and the requirements established on the basis thereof within the time limit determined in accordance with the rules provided in clause 3 of subsection 1³ of § 38 of the Emergency Act. A provider of a vital service is to fulfil the obligation provided in subsections 1 and 2 of this section within the time limits specified in those subsections.

[RT I, 30.12.2025, 4 – entry into force 01.01.2026]

§ 29. Entry into force of Act

(1) This Act enters into force on the day following its publication in *Riigi Teataja*.

(2) Clause 8 of subsection 1 of § 3, subsection 3 of § 3, § 9 and clause 3 of § 23 of this Act enter into force on 1 January 2020.

(3) Clauses 7 and 10 of subsection 1 of § 3, § 21 and clauses 1 and 5 of § 28 of this Act enter into force on 1 January 2022.

¹Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, pp 80–152).
[RT I, 30.12.2025, 4 – entry into force 01.01.2026]