Issuer:	Riigikogu
Type:	act
In force from:	16.08.2022
In force until:	31.12.2026
Translation published:	26.08.2022

Cybersecurity Act[1]

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

Chapter 1
General Provisions

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

(1) This Act provides for requirements for the maintenance of network and information systems essential for the functioning of society, including network and information systems of the public sector, liability and supervision as well as bases for the prevention and resolution of cyber incidents.
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

(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) This Act is not applied to digital service providers which employ on average fewer than 50 persons during a financial year and whose annual balance sheet total or annual turnover does not exceed 10 million euros, taking into account the definitions of micro and small enterprises in European Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.05.2003, pp 36–41).

(4) If the requirements for the maintenance of network and information systems are provided by an international agreement or another Act, this Act is applied with the specifications arising from the international agreement or other Act.

(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) ‘network and information system’ (hereinafter *system*) means an electronic communications network within the meaning of subsection 8 of § 2 of the Electronic Communications Act, any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data, or digital data stored, processed, retrieved or transmitted by aforesaid elements for the purposes of their operation, use, protection and maintenance;
2) ‘security of systems’ means the ability of systems to resist any action that compromises the availability, authenticity, integrity or confidentiality of data processed in the systems or the services offered by, or accessible via, those systems;

2[1]) 'security measures' means organisational, physical and information technological operations or resources applied for achieving and maintaining the security of data and systems;
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]
3) 'cyber incident' means any event in the system compromising or having an adverse effect on the security of the system;
4) 'representative of digital service provider' (hereinafter *representative*) means any 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 a national competent authority or a computer incident response team instead of the digital service provider with regard to the obligations of that digital service provider under this Act;
5) 'online marketplace' means an information society service that allows consumers and traders, for the purposes of the Consumer Protection Act, to conclude online sales or service contracts either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace;
6) 'online search engine' means an information society service that allows users to perform searches of all websites or websites in a particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found;
7) 'cloud computing service' means an information society service that enables access to a pool of flexibly shareable and scalable computing resources without modifying the system;
8) 'computer incident response team' means a group of experts who are tasked with operations supporting the detection, analysis and containment of a cyber incident and the response thereto.

§ 3. Service provider

(1) For the purposes of this Act, 'service provider' means a person who uses a system as follows:
1) a provider of a vital service provided in the Emergency Act upon providing the vital service;
2) an infrastructure manager / railway undertaking provided in the Railways Act who manages public railway infrastructure or whose market share of transport of cargo or transport of passengers forms at least 20 per cent of the market share of transport of cargo or transport of passengers upon providing the service of the functioning of public railways and the functioning of rail transport and public transport of passengers;
3) an aerodrome operator provided in the Aviation Act who operates an aerodrome which is open for international scheduled air traffic and the air navigation service provider who ensures air navigation services in the Tallinn flight information region upon providing the service of the functioning of an aerodrome and air navigation service;
4) a port service provider who is, for the purposes of the Ports Act, the port authority of a port or the port facility authority of a port facility that services ships of a gross tonnage of 500 and more or passenger ships in international marine navigation upon providing the service of the functioning of a port;
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]
5) a communications undertaking provided in the Electronic Communications Act who provides cable distribution services consumed by at least 10,000 end-users and a broadcasting network service provider upon providing cable distribution services or broadcasting network services;
6) an owner of a regional hospital and central hospital of the hospital network provided in the Health Services Organisation Act upon providing in-patient specialised medical care and an owner of an ambulance crew upon providing emergency care;
7) a family physician provided in the Health Services Organisation Act upon providing general medical care;
[RT I, 22.05.2018, 1 – entry into force 01.01.2022]
8) the administrator of the top-level domain name registry associated with the Estonian country code upon providing the service of the system and top-level name server used for the maintenance of the registry;
[RT I, 22.05.2018, 1 – entry into force 01.01.2020]
9) a provider of critical communications services, marine radio communications services and operational communications network services for the purposes of the Electronic Communications Act upon providing those services;
10) Estonian Public Broadcasting upon performing the function provided in clause 10 of subsection 1 of § 5 of the Estonian Public Broadcasting Act.
[RT I, 22.05.2018, 1 – entry into force 01.01.2022]

(2) Service providers specified in subsection 1 of this section who operate in sectors set out in Annex II to Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.07.2016, pp 1–30) are deemed to be operators of essential services for the purposes of said Directive.

(3) Every two years the Estonian Information System Authority identifies the service providers who fall in the scope of this Act and operate in sectors set out in Annex II to Directive (EU) 2016/1148 of the European Parliament and of the Council.
[RT I, 22.05.2018, 1 – entry into force 01.01.2020]

(4) The provisions of this Act concerning service providers are also applied to:
1) a database controller and processor;
2) the Foresight Centre;
3) Eesti Pank (Bank of Estonia);
4) a local authority and a local authorities association;
5) a judicial body;
6) the State Electoral Office;

7) the Chancellery of the Riigikogu;
8) the State Audit Office;
9) the State Forest Management Centre;
10) a legal person governed by public law founded on the basis of law;
11) the Office of the President of the Republic;
12) a governmental authority and a state agency governed by a governmental authority;
13) 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;
14) the Office of the Chancellor of Justice.
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

§ 4. Digital service provider

(1) For the purposes of this Act, 'digital service provider' means an information society service provider provided in the Information Society Services Act who:
1) offers an online marketplace;
2) offers an online search engine; or
3) provides cloud computing services.

(2) A digital service provider who provides services in Estonia but is not established in the European Union must designate a representative in Estonia or in another Member State of the European Union where they provide services and must make the representative's contact details permanently publicly available.

§ 5. Single point of contact and competent authority

The Estonian Information System Authority has the roles of the competent authority referred to in Article 8 (1) of Directive (EU) 2016/1148 of the European Parliament and of the Council and the single contact point referred to in Article 8 (3) and the computer incident response team referred to in Article 9 (1).

§ 5[1]. 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]

§ 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;
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;
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;
4) the principle of cooperation – 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

§ 7. Security measures of service provider's system

(1) A service provider is to permanently apply security measures:
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]
1) for preventing cyber incidents;
2) for resolving cyber incidents;
3) for preventing and mitigating an impact on the continuity of the service or the security of the system due to a cyber incident or for preventing and mitigating a possible impact on the continuity of another dependant service or the security of a system.

(2) Upon the application of security measures, the service provider is required to:
1) prepare a system risk assessment in which they must set out a list of risks affecting the security of the system and the continuity of the service and causing the occurrence of cyber incidents, determine the severity of consequences of a cyber incident occurring upon the realisation of risks, and describe the measures for resolving a cyber incident;
2) ensure the existence and timeliness of a documented system risk assessment, security regulations and description of the application of security measures;
3) ensure the monitoring of the system for detecting actions or software compromising its security and communicate information about the actions or software compromising the security of the system to the Estonian Information System Authority;
4) take measures for reducing the impact and spread of a cyber incident, including restriction of the use of or access to the system, where necessary.
5) [repealed – RT I, 06.08.2022, 2 – entry into force 16.08.2022]
6) [repealed – RT I, 06.08.2022, 2 – entry into force 16.08.2022]

(3) If the service provider authorises another party to administer the system or uses another party to host the system, the service provider is responsible for the application of the security measures of the system by the other party.

(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]

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

(1) A service provider informs the Estonian Information System Authority immediately but no later than 24 hours after becoming aware of a cyber incident:
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.

(1^1) If a service provider authorises another party to administer a system or uses another party to host a system, the service provider is responsible for ensuring that the other party informs the service provider no later than 24 hours after becoming aware of a cyber incident specified in subsection 1 of this section.
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

(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 degree of consequences determined in the system risk assessment prepared on the basis of clause 1 of subsection 2 of § 7 of this Act;
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;
4) the extraordinary measures set out in the system risk assessment prepared under clause 1 of subsection 2 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 resolving the cyber incident;
5) the service provider, the provider of another service or service users suffer or may suffer significant damage due to the cyber incident.

(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) The obligation provided in subsection 1 of this section does not restrict the right of the service provider to notify the Estonian Information System Authority of a cyber incident that does not have a significant impact provided in subsection 2 of this section.

(5) Within a reasonable period of time, the service provider is required to notify persons possibly affected by a cyber incident with a significant impact or the public if the persons affected cannot be notified individually.

(6) If the service provider does not perform the notification obligation provided in subsection 5 of this section within a reasonable period of time, the Estonian Information System Authority may notify the person affected or the public itself, also informing the service provider of such notification.

(7) In resolving a cyber incident with a significant impact, the service provider is required to send the Estonian Information System Authority a report which includes information about the causes for the cyber incident, the time spent on its resolution, the measures applied and the impact of the cyber incident.

(8) The procedure for notifying of a cyber incident and the format of the report may be established by a regulation of the minister in charge of the policy sector.

(9) The service provider is required to notify the Estonian Information System Authority of the significant impact of a cyber incident concerning a digital service provider on the continuity of their service if their service depends on the service of the digital service provider defined in § 4 of this Act.

§ 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

(1) A digital service provider is required to ascertain the risks posed to the security of their system and analyse them and take organisational and technical measures appropriate for risk management.

(2) In choosing measures for ensuring the security of a system the following must be taken into account:
1) the security of the technical infrastructure;
2) the prevention, detection and resolution of a cyber incident;
3) continuity management;
4) monitoring, auditing and testing;
5) compliance with international standards.

(3) In applying subsection 2 of this section, the digital service provider is required to abide by the implementing regulation of the European Commission issued under Article 16 (8) of Directive (EU) 2016/1148 of the European Parliament and of the Council.

(4) The digital service provider takes appropriate measures to minimise the impact of a cyber incident on the continuity of the service provided.

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

(1) A digital service provider notifies the competent authority or the computer security incident response team of a cyber incident which has a significant impact on the digital service provided, immediately after becoming aware of the cyber incident.

(2) A notification must be submitted to the competent authority or the computer security incident response team of the Member State where:
1) the digital service provider is founded;
2) the parent company of the group is founded in the case of a group; or
3) the representative appointed by an economic operator from a third country is located.

(3) Notifying of a cyber incident is based on the criteria provided in the implementing regulation of the European Commission issued under Article 16 (8) of Directive (EU) 2016/1148 of the European Parliament and of the Council.

(4) The notification must include information enabling the competent authority or the computer security incident response team to determine any cross-border impact of the cyber incident.

(5) If a cyber incident has a significant impact on the continuity of a digital service in another Member State, the Estonian Information System Authority notifies the affected Member State on the basis of the information presented by the digital service provider.

(6) If for the purpose of preventing a cyber incident or resolving an on-going cyber incident and in the public interest it is necessary to notify the public, the Estonian Information System Authority may, after informing the digital service provider, notify the public of the cyber incident or require the digital service provider to do so.

(7) Subsection 1 of this section is not applied if the digital service provider lacks information for identifying the significance of the impact of the cyber incident.

Chapter 3
Ensuring Cybersecurity

§ 12. Prevention and resolution of cyber incident

(1) Ensuring cybersecurity and preventing and resolving 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 resolving 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.

(4) The Estonian Information System Authority has the right to forward to a foreign state or the European Union Agency for Network and Information Security or another organisation information related to preventing and resolving a cyber incident for the performance of the functions provided in § 5 of this Act or an obligation arising from European Union law or in cases and pursuant to the procedure set forth in an international agreement provided the information forwarded does not harm national security or criminal proceedings.

(5) When forwarding information, the Estonian Information System Authority takes into account the business interests of the service provider or digital service provider and abides by the obligation to keep business secrets.

§ 13. Cyber incident registry

(1) The cyber incident registry (hereinafter the *registry*) is a database maintained by the Estonian Information System Authority where data describing the occurrence of a cyber incident is entered for the purpose of keeping record of cyber incidents and analysing cyber incidents for resolving them, forwarding alerts and performing supervisory operations.

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

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

Chapter 3^1
Cybersecurity Certification

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

§ 13^1. National cybersecurity certification authority

For the purposes of Article 58(1) 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), the national cybersecurity certification authority is the Consumer Protection and Technical Regulatory Authority.
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

§ 13^2. 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) State supervision over the compliance with the requirements set for digital service providers by §§ 10 and 11 of this Act is exercised if the Estonian Information System Authority is notified of said requirements not being complied with by:
1) a digital service provider established in Estonia;
2) a digital service provider belonging to a group whose parent company is established in Estonia;
3) a digital service provider of a third country who has a representative in Estonia.

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

§ 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) Upon exercising state supervision over compliance with the requirements of §§ 7 and 8 of this Act and legislation established on the basis of said sections, law enforcement agencies may also apply, in addition to the special measures referred to in subsection 1 of this section, 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.

§ 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.

(1^1) 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, 06.08.2022, 2 – entry into force 16.08.2022]

(2) The addressee and in the case of a service provider set out in clause 1 of subsection 1 of § 3 of this Act the authority organising the continuity of the vital service must be notified of the application of a measure provided in this section at the first opportunity.

(3) It is required to record the measure provided for 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.

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

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

§ 17[1]. Rate of non-compliance levy

Upon failure to comply with a compliance notice in the course of state supervision proceedings, 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 20,000 euros.
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

§ 17[2]. 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 90thday 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]

Chapter 5
Liability

§ 18. Violation of requirements of Act

(1) Violation of the requirements provided in subsections 1–3 of § 7 of this Act
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.

§ 18[1]. 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]

§ 19. Proceedings

(1) The body conducting extra-judicial proceedings pertaining to the misdemeanour provided in § 18 of this Act is the Estonian Information System Authority.

(2) If the misdemeanour provided in § 18 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.

(3) The body conducting extra-judicial proceedings pertaining to the misdemeanour provided in § 18[1] of this Act is the Consumer Protection and Technical Regulatory Authority.
[RT I, 06.08.2022, 2 – entry into force 16.08.2022]

Chapter 6

Implementing Provisions

§ 20. Identification of service providers

The service providers referred to in subsection 3 of § 3 of this Act are identified by the Estonian Information System Authority by 9 November 2018.

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

§ 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.

[1]Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.07.2016, pp 1–30).