Issuer:	Riigikogu
Type:	act
In force from:	23.05.2018
In force until:	In force
Translation published:	23.05.2018

Cybersecurity Act[1]

Passed 09.05.2018

Chapter 1
GENERAL PROVISIONS

§ 1. Subject matter and scope of Act

(1) This Act provides for the requirements for the maintenance of network and information systems essential for the functioning of society and state and local authorities' network and information systems, liability and supervision as well as the bases for the prevention and resolution of cyber incidents.

(2) This Act is not applied to the processing of state secrets and classified information of foreign states or to the maintenance of processing systems for such information.

(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 for 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 2 (8) 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;
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 for in the Emergency Act upon providing the vital service;
2) an infrastructure manager / railway undertaking provided for 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 percent 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 for 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 owns a port provided for in the Ports Act which services passenger ships in international marine navigation or ships of a gross tonnage of 500 and more, and a port which services category I ships which navigate in internal water bodies or class A passenger ships defined pursuant to the Maritime Safety Act upon providing the service of the functioning of a port;
5) a communications undertaking provided for 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 for 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 for in the Health Services Organisation Act upon providing general medical care;
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;
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 for in clause 5 (1) 10) of the Estonian Public Broadcasting Act.

(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 shall identify 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.

(4) The provisions of this Act concerning service providers are also applied to state and local authorities with the specifications provided for in § 9 of this Act.

§ 4. Digital service provider

(1) For the purposes of this Act, ‘digital service provider’ means an information society service provider provided for 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 shall designate a representative in Estonia or in another Member State of the European Union where they provide services and shall make the representative’s contact details permanently publicly available.

§ 5. Single point of contact and competent authority

The Estonian Information System Authority shall have 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).

§ 6. Principles of ensuring cybersecurity

The following principles shall be taken into account in ensuring cybersecurity:
1) the principle of personality – ensuring the security of a system shall be arranged by the service provider;
2) the principle of integral protection – the service provider shall ascertain potential risks posed to the system and apply 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 shall apply due care and measures to avoid the escalation of the effect of the cyber incident and its possible spread to another system and shall notify the supervisory authority provided for in this Act of the cyber incident;
4) the principle of cooperation – in ensuring cybersecurity and resolving cyber incidents the parties shall cooperate and, if necessary, take into account the mutual connection between and dependence of the systems and services.

Chapter 2
OBLIGATIONS FOR ENSURING CYBERSECURITY

§ 7. Security measures of service provider's system

(1) A service provider shall permanently apply organisational, physical and information technological security measures:
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 shall 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, if necessary;
5) check the sufficiency and compliance of the application of security measures and document the results;
6) preserve the documents provided for in clause 5) of this subsection no less than three years as of the creation thereof.

(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) The description of the security measures of the system used for the provision of a service and the requirements for the preparation of a risk assessment shall be established by a regulation of the minister responsible for the area.

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

(1) A service provider shall inform 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.
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 7 (2) 1) 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 7 (2) 1) 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 for 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 for in subsection (2) of this section.

(5) Within a reasonable period of time, the service provider is required to notify persons possibly affected by the 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 for 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 responsible for the area.

(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

(1) In the administration of a state and local authority's system, the obligations provided for in subsections 7 (1) through (3) of this Act and the requirements for notifying of a cyber incident provided for in § 8 shall apply.

(2) Ensuring the security of a system specified in subsection (1) of this section is subject to the requirements provided for in the regulation established under clause 439 (1) 4) of the Public Information Act.

(3) A list of systems necessary for international military cooperation within the area of government of the Ministry of Defence and their security requirements shall be established by a regulation of the minister responsible for the area.

§ 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 shall 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 shall take 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 shall notify 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 shall 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 shall be based on the criteria provided for 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 shall include information enabling the competent authority or the computer security incident response team 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 shall notify 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 shall be coordinated 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 for 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 shall take into account the business interests of the service provider or digital service provider and shall abide 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 shall be established by a regulation of the minister responsible for the area.

Chapter 4
STATE AND ADMINISTRATIVE SUPERVISION

§ 14. Exercise of state and administrative supervision

(1) State and administrative supervision over the compliance with the requirements provided for in this Act and in legislation established on the basis of this Act are 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) Administrative supervision over the compliance with the system requirements provided by the regulation established under subsection 9 (3) of this Act is exercised by the Ministry of Defence and the Estonian Defence Forces.

§ 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 for in §§ 30, 31, 32, 49, 50 and 51 of the Law Enforcement Act on the basis and pursuant to the procedure provided for in the Law Enforcement Act.

(2) Upon exercising state supervision over the 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 for in § 52 of the Law Enforcement Act on the basis and pursuant to the procedure provided for 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.

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

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

Chapter 5
LIABILITY

§ 18. Violation of requirements of Act

(1) Violation of the requirements provided for in subsections 7 (1) through (3) 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.

§ 19. Proceedings

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

(2) If the misdemeanour provided for 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.

Chapter 6
IMPLEMENTING PROVISIONS

§ 20. Identification of service providers

The service providers referred to in subsection 3 (3) of this Act shall be 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 3 (1) 8), subsection 3 (3), § 9 and clause 23 3) of this Act enter into force on 1 January 2020.

(3) Clauses 3 (1) 7) and 10), § 21 and clauses 28 1) and 5) 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).

Eiki Nestor
President of the Riigikogu