**Section 31.**

**National Cybersecurity Law**

**Chapter I**

**General Provisions**

**Section 1. Terms Used in this Law**

* The following terms are used in the Law:

1) **CSIRT network**– a network of computer security incident response teams of the European Union Member States;

2) **data centre**– a structure or a group of structures dedicated to the centralised accommodation, interconnection, and operation of information technology and electronic communications network equipment providing data storage, processing, and forwarding (transport) services and also all the facilities and infrastructures for power distribution and environmental control, and also the necessary resilience and security level necessary for ensuring the availability of the service according to the requirements brought forward;

3) **near miss**– an event that could have compromised the availability, authenticity, integrity, or confidentiality of processed data or of the services offered by, or accessible via, network and information systems, but that was successfully prevented from materialising or that did not materialise;

4) **vulnerability**– a security flaw of information and communication technologies or their services which is a systemic weakness caused during the course of establishment, maintenance, or modification of the information system or electronic communications network, resulting in a threat to the confidentiality, integrity, or availability of information and communication technologies, and which can be exploited for the implementation of a cyberattack;

5) **information and communication technologies**– technologies which carry out electronic processing, including creation, modification, deletion, storage, representation, forwarding, or transmission of information (hereinafter – electronic processing) for the fulfilment of the tasks intended for them with the help of technical aids and ensure mutual communication of technology users;

6) **cyber threat**– any potential circumstance, event, or action that could damage, disrupt, or otherwise adversely impact network and information systems, the users of such systems and other persons as defined in Article 2(8) of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 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) (hereinafter – Regulation 2019/881);

7) **cybersecurity**– the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats as defined in Article 2(1) of Regulation 2019/881;

8) **cybersecurity incident** (hereinafter – the cyber incident) – an event compromising the availability, integrity, authenticity, or confidentiality of processed data or of the services offered by, or accessible via, network and information systems;

9) **cyber incident handling**– any actions and procedures aiming to prevent, detect, analyse, and contain or to respond to and recover from a cyber incident;

10) **cyber risk**– the potential for loss or disruption caused by a cyber incident on services according to the potential consequences and the likelihood of occurrence of them setting in;

11) **cyberattack**– an active act by attackers to disrupt the confidentiality, integrity, or availability of data and service of information and communication technologies;

12) **cyber hygiene**– an aggregate of intentional everyday practices and habits implemented for the purpose of preventing cyber threats and ensuring data protection, and retaining the availability, integrity, and confidentiality of information and communication technologies;

13) **large performer of economic activity**– a legal or natural person, or an association of such persons, which or who performs economic activity in the Republic of Latvia and conforms to at least one of the following features:

a) the performer of economic activity employs at least 250 employees;

b) the total net turnover of the last financial year of the performer of economic activity in the world exceeds EUR 50 million and the annual balance sheet total exceeds EUR 43 million;

14) **denial of service cyberattack**– an attack made against the infrastructure of the service provider aiming at disruption of the availability of the service;

15) **cross-border cyber incident**– an incident causing a level of disruption which exceeds the capacity of a Member State to respond or which has an essential impact on at least two Member States;

16) **small performer of economic activity**– a legal or natural person, or an association of such persons, which or who performs economic activity in the Republic of Latvia and conforms to all of the following features:

a) the performer of economic activity employs not more than 49 employees;

b) the total net turnover of the last financial year of the performer of economic activity in the world or the annual balance sheet total does not exceed EUR 10 million;

17) **National Cybersecurity Strategy**– a strategic planning document which lays down the basic principles for cybersecurity policy-making, the objective and strategic priorities thereof in accordance with the provisions of Section 42 of this Law;

18) **NIS Cooperation Group**– the Network and Information Systems Cooperation Group of the European Union;

19) **significant cyber threat**– a cyber threat which, taking into account its technical properties, may be considered as capable of seriously disrupting the network and information systems of any legal or natural person or recipients of services provided by such person, causing considerable material or non-material damage;

20) **significant cyber incident**– a cross-border cyber incident or such cyber incident which has an impact on the continuity of the service provided or on public interests and which meets the criteria referred to in Section 31, Paragraph one of this Law;

21) **network**:

a) an electronic communications network;

b) any device or a group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of digital data; or

c) digital data stored, processed, retrieved or transmitted by elements covered under Sub-clauses “a” and “b” for the purposes of their operation, use, protection, and maintenance;

22) **trust service**– an electronic service within the meaning of Article 3(16) of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC;

23) **unified national internet exchange point**– a constant aggregate of physical infrastructure and services which is established and maintained in order to ensure unified national internet exchange;

24) **medium performer of economic activity**– a legal or natural person, or an association of such persons, which or who performs economic activity in the Republic of Latvia and conforms to all of the following features:

a) the performer of economic activity is not a small performer of economic activity;

b) the performer of economic activity employs not more than 249 employees;

c) the total net turnover of the last financial year of the performer of economic activity in the world does not exceed EUR 50 million or the annual balance sheet total does not exceed EUR 43 million.

**Section 2. Purpose of the Law**

* The purpose of the Law is:

1) to improve security of information and communication technologies, including by laying down the requirements for the provision and receipt of essential and important services, and also for the operation of information and communication technologies;

2) to determine the procedures for ensuring cybersecurity, providing for the division of responsibility and the competence of the National Cybersecurity Centre, the framework of cooperation, and the tasks for the promotion of cybersecurity;

3) to promote the implementation of cybersecurity measures in a way to be able to foresee and prevent, and also to overcome cyber threat in a timely manner and to liquidate its consequences, ensuring continuity of confidentiality, integrity, and availability of services to the extent possible.

**Section 3. Scope of Application of the Law**

* (1) The Law shall apply to:

1) providers of essential services, providers of important services, and owners and legal possessors of the critical infrastructure of information and communication technologies (all together hereinafter – the subjects);

2) institutions of direct and indirect administration, derived public entities, and other State authorities, and also legal persons governed by private law which are carrying out a task delegated by the public administration (all together hereinafter – the State and local government authorities), except for State security institutions;

3) legal persons governed by private law;

4) in the cases specified in this Law – to natural persons who participate in the process of coordinated vulnerability discovery.

* (2) The Law shall not apply to the content of the information to be transmitted in electronic communications networks, including to the content of services of an information society and audiovisual works if they are not used as a component of cyber incidents.
* (3) The Law shall apply to financial entities within the meaning of Article 2(2) of Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (hereinafter – Regulation 2022/2554), except for cases if it has been laid down otherwise in Regulation 2022/2554 and other laws and regulations regarding cybersecurity of financial entities, including other special requirements in relation to risk management (management of risks related to the third parties, operational resilience, testing, and incident reports). The Law shall not apply to the financial entities which have been excluded from the scope of Regulation 2022/2554 in accordance with Article 2(4) of Regulation 2022/2554.
* (4) If sector-specific European Union legal acts provide for taking cybersecurity risk management measures for the providers of essential services or providers of important services or to report on cyber incidents and, if in terms of impact such requirements are at least equal to the obligations specified in this Law, the relevant conditions of this Law, including in Part VII of this Law regarding supervision and enforcement, shall not be applied to these subjects. If sector-specific European Union legal acts do not apply to all providers of essential services and providers of important services in a specific sector, the application of the relevant requirements of this Law shall be continued in relation to the providers of essential services and providers of important services to which the abovementioned sector-specific European Union legal acts do not apply.
* (5) The requirements referred to in Paragraph four of this Section shall be considered as equivalent in terms of impact to the measures specified in this Law if:

1) in terms of impact, the cybersecurity risk management measures are at least equivalent to the requirements laid down in Sections 21, 22, and 23 of this Law; or

2) the sector-specific European Union legal act provides for immediate and, in the relevant case, automatic and direct access for the computer security incident response teams specified in Section 9 of this Law, the competent authorities specified in Section 12 of this Law, and the national competent authority specified in Section 4, Paragraph one of this Law to reports on cyber incidents and if, in terms of impact, the requirements for reporting on cyber incidents are at least equivalent to the requirements laid down in Section 29 of this Law.

**Chapter II**

**Authorities Responsible for Cybersecurity**

**Section 4. National Cybersecurity Centre**

* (1) The National Cybersecurity Centre is the national competent authority which operates as the single point of contact in cybersecurity issues and implements national cybersecurity supervision, forms initiatives of the national cybersecurity action policy, and, within the scope of its competence, forms and implements international cooperation in the field of cybersecurity.
* (2) The Ministry of Defence shall implement the functions of the National Cybersecurity Centre.

**Section 5. Tasks of the National Cybersecurity Centre**

* (1) The National Cybersecurity Centre shall have the following tasks:

1) to coordinate cooperation with the competent institutions and single points of contact of other European Union Member States, the European Commission, the European Union Agency for Cybersecurity, and other competent authorities of the European Union in cybersecurity issues;

2) to cooperate with the providers of essential services and providers of important services for determination of the security level of their information systems;

3) to implement supervisory functions, including to supervise how the providers of essential services and providers of important services are fulfilling the obligations specified in this Law;

4) to assess the conformity of the cyber risk management measures of the providers of essential and important services with the requirements laid down in laws and regulations;

5) to supervise the conformity with the security requirements for public electronic communications networks;

6) to maintain the list of providers of essential and important services compiled by State institutions and self-identified, to ensure the approval thereof with the Supervisory Committee of Digital Security, and also to submit information which has been compiled and, if necessary, anonymised to the competent authorities of the European Union on the identified providers of essential and important services;

7) to ensure the functions of the National Cybersecurity Council and the Supervisory Committee of Digital Security;

8) to assess the conformity of the development projects of State information systems and information systems of authorities with the minimum cybersecurity requirements in conformity with the provisions of the Law on State Information Systems;

9) to ensure the operation of the unified national internet exchange point and also to coordinate receipt of services of the unified national internet exchange point in cooperation with State security institutions;

10) in cooperation with State administration institutions, State security institutions, and representatives of the private sector, to develop the National Cybersecurity Strategy and, not later than three months after approval of the National Cybersecurity Strategy, to inform the European Commission thereof;

11) to ensure the development of the plan referred to in Section 31, Paragraph three of this Law and to integrate it in national defence plans, to participate in the European Cyber Crises Liaison Organisation Network;

12) to cooperate with the European Union Agency for Cybersecurity and to inform it, without delay, of cross-border cyber incidents which affect providers of essential or important services, and also to provide a report thereto, once in three months, on all significant cyber incidents which have occurred, cyber incidents, near misses, and cyber threats of which the subjects have notified in accordance with the provisions of Section 29 of this Law;

13) to cooperate with the competent institutions of other European Union Member States, including to send the information received in accordance with Section 29 of this Law to them on significant cyber incidents affecting these European Union Member States upon request of the computer security incident response team;

14) to coordinate the cross-border cyber incident handling in cooperation with the computer security incident response teams, the European Union, foreign, and international competent authorities;

15) to cooperate with the NIS Cooperation Group and to implement the tasks related thereto;

16) to implement the rights and obligations specified for the National Coordination Centre in Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres;

17) to maintain a unified depiction of the activities occurring in the cyberspace of Latvia, except for the content of the information transmitted therein;

18) to inform the public of current cyber threats;

19) to ensure the operation of security operations centres in the data centres referred to in Section 25, Paragraph one of this Law;

20) within the scope of its competence, to participate in the process of coordinated vulnerability discovery and prevention in accordance with the provisions of Chapter VI of this Law;

21) as necessary, to inform the European Union Agency for Cybersecurity of the information to be included in the database of vulnerabilities;

22) in cases when vulnerability also affects another European Union Member State, to cooperate with the competent authorities of this Member State;

23) as necessary, to participate in assessment of the cybersecurity capacity and action policy of European Union Member States in the status of an independent expert.

* (2) The National Cybersecurity Centre shall implement the tasks referred to in Paragraph one, Clauses 2, 3, and 4 of this Section only in relation to those providers of essential services and providers of important services which are not owners or legal possessors of the critical infrastructure of information and communication technologies.
* (3) The Ministry of Defence shall delegate the fulfilment of the tasks of the National Cybersecurity Centre referred to in Paragraph one, Clauses 17–23 of this Section to the Institute of Mathematics and Computer Science of the University of Latvia, entering into a delegation contract.

**Section 6. Rights of the National Cybersecurity Centre**

* (1) The National Cybersecurity Centre has the following rights:

1) to perform the supervision of cybersecurity of providers of essential services and providers of important services in relation to the fulfilment of the specified obligations;

2) to request and receive information from providers of essential and important services on the information and communication technologies in their ownership and possession and also on the implemented and planned cybersecurity and cyber risk management measures, cyber incidents, near misses, cyber threats, and vulnerabilities;

3) to request and receive information from the State and local government authorities at their disposal on providers of essential and important services;

4) to provide instructions to ensure the fulfilment of the obligations specified in this Law for the providers of essential services and providers of important services;

5) to take a decision (also to issue an administrative act) to ensure the fulfilment of the obligations specified in this Law or to prevent national security or cyber threat;

6) to perform the forced execution of legal obligation in accordance with Section 41 of this Law;

7) to request and receive information from operators of data centres on the fulfilment of the obligations specified in Section 25 of this Law.

* (2) The Constitution Protection Bureau shall implement the rights referred to in Paragraph one, Clauses 1 and 2 of this Section in relation to the critical infrastructure of information and communication technologies, including the providers of essential services and providers of important services which are owners or legal possessors of the critical infrastructure of information and communication technologies. The National Cybersecurity Centre shall implement the rights referred to in Paragraph one, Clauses 5 and 6 of this Section in relation to the critical infrastructure of information and communication technologies in cooperation with the Constitution Protection Bureau in accordance with the provisions of Chapter VII of this Law.

**Section 7. Tasks of the Constitution Protection Bureau**

* The Constitution Protection Bureau shall have the following tasks:

1) to implement supervisory functions, including to supervise how the owners and legal possessors of the critical infrastructure of information and communication technologies are fulfilling the obligations specified in this Law;

2) to cooperate with the owners and legal possessors of the critical infrastructure of information and communication technologies for determination of the security level of their information systems;

3) to coordinate the cross-border cyber incident handling in cooperation with computer security incident response teams;

4) to assess the conformity of the cyber risk management measures to be implemented by the owners and legal possessors of the critical infrastructure of information and communication technologies with the requirements laid down in laws and regulations.

**Section 8. Rights of the Constitution Protection Bureau**

* The Constitution Protection Bureau has the following rights:

1) to perform cybersecurity supervision of the owners and legal possessors of the critical infrastructure of information and communication technologies;

2) to request and receive information from the owners and legal possessors of the critical infrastructure of information and communication technologies on the information and communication technologies in their ownership and possession and also on the implemented and planned cybersecurity and cyber risk management measures, cyber incidents, near misses, cyber threats, and vulnerabilities;

3) to provide instructions to ensure the fulfilment of the obligations specified in this Law for the owner and legal possessor of the critical infrastructure of information and communication technologies or to prevent threat to national security.

**Section 9. Computer Security Incident Response Teams**

* (1) Computer security incident response teams are authorities which provide support to the State and local government authorities in the field of cybersecurity, maintain and update information on cyber threats, and provide support to natural and legal persons in prevention of cyber incidents.
* (2) The tasks of computer security incident response teams shall be performed by:

1) the Military Intelligence and Security Service with regard to the Ministry of Defence, institutions subordinate thereto, and the National Armed Forces;

2) the Institute of Mathematics and Computer Science of the University of Latvia with regard to the State and local government authorities (except for State security institutions and that specified in Clause 1 of this Paragraph) and also legal persons governed by private law.

* (3) The Institute of Mathematics and Computer Science of the University of Latvia shall perform the tasks assigned thereto and implement the rights under subordination of the Ministry of Defence in accordance with the provisions of this Law.
* (4) The Cabinet shall determine the requirements for computer security incident response teams.

**Section 10. Tasks of Computer Security Incident Response Teams**

* Computer security incident response teams shall have the following tasks:

1) to conduct analysis at the State level of significant cyber threats, vulnerabilities, and cyber incidents;

2) to respond to cyber incidents, upon request of the subject to provide support in cyber incident handling or to coordinate the prevention of a cyber incident;

3) to warn and provide the National Cybersecurity Centre, the Constitution Protection Bureau, the subjects, and, as necessary, other institutions with the relevant information on current significant cyber incidents, cyber incidents, near misses, cyber threats, and vulnerabilities;

4) to organise educating measures, to perform analytical and research work, and to organise thematic training in the field of cybersecurity;

5) to provide support to State authorities in the protection of State security and also detection (investigation) of criminal offences and other violations of the law in the field of information and communication technologies;

6) to cooperate with the competent institutions of the European Union, foreign, and international organisations and computer security incident response teams, to participate in the CSIRT network;

7) without delay, to inform the National Cybersecurity Centre and State security institutions of the significant cyber incident referred to in Section 30, Paragraph one of this Law and also to inform the competent institution of another European Union Member State of the significant cyber incident which disrupts the continuity of operation of an essential or important service in the particular Member State;

8) to inform the National Cybersecurity Centre and the Constitution Protection Bureau of the detected non-conformity of information and communication technologies of the subject with the laws and regulations laying down the cybersecurity requirements and also of the detected cases when the subject has not notified of a cyber incident in accordance with Section 29 of this Law;

9) within the scope of its competence, to cooperate with the State and private sector authorities in order to facilitate cybersecurity and cyber resilience, to cooperate and exchange the relevant information on current cyber threats with the communities of the subjects;

10) upon request of the subject, to perform proactive scanning of networks and information systems of the subject to disclose vulnerabilities with potential essential impact;

11) to fulfil other obligations specified in laws and regulations.

**Section 11. Rights of Computer Security Incident Response Teams**

* (1) Computer security incident response teams are entitled:

1) to request and receive the following from the subjects, the State and local government authorities, and legal persons governed by private law:

a) information on the introduced security requirements of information and communication technologies (including networks and information systems), the identified vulnerabilities and cyber threat;

b) technical information on a cyber incident that has occurred or is occurring (information on the scope of the cyber incident, malicious software files that have caused the cyber incident, description of vulnerabilities, technical measures taken for the prevention of the cyber incident, information on activities performed by persons doing harm or other technical information, including IP addresses);

2) to obtain from the subjects, the State and local government authorities, and legal persons governed by private law, upon mutual agreement, online data flow for the identification and prevention of cyber threat;

3) to perform inspections in the infrastructure of information and communication technologies of the providers of essential and important services, except for the critical infrastructure of information and communication technologies;

4) upon request of the Constitution Protection Bureau, to perform inspections in the critical infrastructure of information and communication technologies;

5) to request that the National Cybersecurity Centre sends information to the competent authority of a European Union Member State, the NIS Cooperation Group, the CSIRT network, or the European Union Agency for Cybersecurity on a cyber incident which has an impact on the provision of essential or important services in the particular Member State;

6) to carry out proactive non-intrusive scanning of publicly available networks and information systems in order to detect vulnerabilities or insecure configurations and to inform the relevant subjects thereof.

* (2) The computer security incident response team shall carry out the scanning referred to in Paragraph one, Clause 6 of this Section in a way as not to disrupt the continuity of the service provision of the relevant subject. Scanning in the critical infrastructure of information and communication technologies shall be carried out in agreement with the Constitution Protection Bureau.

**Section 12. Cooperation of the Competent Authorities**

* (1) The National Cybersecurity Centre, the Constitution Protection Bureau, and computer security incident response teams shall, as necessary and regularly but not less than once in a quarter, mutually exchange information on topicalities in the field of cyber incidents.
* (2) The National Cybersecurity Centre and the Constitution Protection Bureau shall, as necessary and regularly but not less than once in a quarter, mutually exchange information on topicalities in supervision of the subjects, including in relation to the identification of the subjects, cyber risks, cyber threats, cyber incidents, near misses, and also security risks, threats, and incidents not related to cybersecurity which affect the subjects unless exchange of such information is in contradiction with the interests of national security.
* (3) The National Cybersecurity Centre and the Constitution Protection Bureau shall, as necessary and regularly but not less than twice in a year, exchange information on the current cyber incidents and cyber threats of the financial sector with Latvijas Banka, the Public Utilities Commission, and the Supervisory Committee of Digital Security unless exchange of such information is in contradiction with the interests of national security.
* (4) Computer security incident response teams shall, within the scope of their competence, cooperate with:

1) Latvijas Banka in the issues related to cybersecurity of the financial entities referred to in Article 2 of Regulation 2022/2554, including provide information at the disposal thereof to Latvijas Banka on the detected cyber incidents in the infrastructure of information and communication technologies of the subjects referred to in Section 16, Paragraph one, Clause 8, Sub-clause “n” of this Law;

2) the Public Utilities Commission in issues affecting cybersecurity of electronic communications merchants, including provide information at the disposal thereof to the Public Utilities Commission which is necessary thereto for the implementation of the functions specified in the Electronic Communications Law;

3) the Civil Aviation Agency for the implementation of the supervisory functions specified in Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 and Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 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;

4) the State Data Inspectorate in issues related to personal data protection, including provide information at the disposal thereof to the State Data Inspectorate on violations of personal data protection;

5) the competent institutions of the police, the Office of the Prosecutor, the court, and other competent institutions for the prevention, detection, and investigation of criminal offences. In case if a computer security incident response team detects that a cyber incident, near miss, cyber threat, or vulnerability *prima facie* displays the signs of a criminal offence, the computer security incident response team shall, without delay, inform the competent institution thereof, providing thereto the information at the disposal thereof which is necessary for the performance of procedural activities;

6) State security institutions in issues related to national security, including provide information at the disposal thereof to the competent State security institutions on cyber incidents, near misses, cyber threats, and vulnerabilities which endanger or may potentially endanger national security.

* (5) The Institute of Mathematics and Computer Science of the University of Latvia shall provide the Military Intelligence and Security Service with the information at its disposal on cyber incidents in the Ministry of Defence, the institutions subordinate thereto, and the National Armed Forces.
* (6) The Military Intelligence and Security Service shall provide information to the Institute of Mathematics and Computer Science of the University of Latvia in order for it to ensure the implementation of the tasks specified in Section 10, Clause 5 of this Law and also other information at its disposal on cyber incidents within the competence of the Institute of Mathematics and Computer Science of the University of Latvia.

**Section 13. Cooperation with the Authorities Responsible for Cybersecurity**

* The subjects, the State and local government authorities, and legal persons governed by private law have the obligation to cooperate with computer security incident response teams, the National Cybersecurity Centre, and the Constitution Protection Bureau, providing them with the necessary information and meeting the lawful requirements thereof.

**Section 14. National Cybersecurity Council**

* (1) The National Cybersecurity Council is a collegial authority which coordinates the development of the policy related to cybersecurity and also the planning and implementation of relevant tasks and measures.
* (2) The composition of the National Cybersecurity Council shall be determined by the Prime Minister.

**Section 15. Supervisory Committee of Digital Security**

* (1) The Supervisory Committee of Digital Security is a collegial supervisory authority under subordination of the Minister for Defence.
* (2) The by-laws of the Supervisory Committee of Digital Security shall be approved by the Cabinet.
* (3) Computer security incident response teams shall, within the scope of their competence, cooperate and provide the information necessary for the implementation of the functions of the Supervisory Committee of Digital Security, including inform of the detected significant cyber incidents and cyber threats which affect qualified trust service providers or qualified trust services provided thereby.

**Chapter III**

**Identification and Recording of the Subjects**

**Section 16. Provider of Essential Services**

* Within the meaning of this Law, a provider of essential services is:

1) the maintainer of the top level domain “.lv” register and the electronic numbering system;

2) the provider of domain name registration and domain name system services;

3) an electronic communications merchant;

4) a qualified trust service provider;

5) an institution of direct administration and another State authority, and also a legal person governed by private law which is fulfilling a task delegated by the State administration, except for State security institutions;

6) a derived public entity;

7) public media;

8) a large performer of economic activity which is:

a) an energy supply merchant;

b) a petroleum supply merchant;

c) a hydrogen supply merchant;

d) an air navigation service provider;

e) an aircraft operator;

f) an aerodrome operator or an operator of other civil aviation objects and facilities;

g) a railway undertaking;

h) a railway infrastructure manager;

i) a shipping company, excluding individual ships managed by this company;

j) a port authority;

k) a merchant which performs commercial activity in the port area;

l) a merchant which manages State motor roads or performs the maintenance works of the State motor road infrastructure;

m) an operator of intelligent transport systems;

n) a credit institution, a central counterparty, or a trading venue (within the meaning of the Financial Instrument Market Law);

o) a medical treatment institution;

p) a reference laboratory of the European Union;

q) a pharmacy merchant;

r) a manufacturer of critical medical devices (in accordance with that specified in Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on a reinforced role for the European Medicines Agency in crisis preparedness and management for medicinal products and medical devices);

s) a supplier or distributor of drinking water (except if the principal activity of the merchant is not related to the distribution of drinking water);

t) a water management service provider;

u) an internet exchange point service provider;

v) a cloud computing service provider;

w) a data centre service provider;

x) a content delivery network service provider;

y) an information and communication technologies management or cybersecurity service provider;

z) a space-based service provider or an operator of the infrastructure to be used for the provision of such services;

9) a performer of economic activity which performs economic activity in at least one of the fields referred to in Paragraph one, Clause 8 of this Section and is the only provider of such service in the Republic of Latvia;

10) an institution of indirect administration which provides services or operates in the field of private law in at least one of the fields referred to in Paragraph one, Clause 8 of this Section;

11) a performer of economic activity which provides a service the disruption of which might significantly affect public safety, national defence, or public health or also cause a significant systemic risk, particularly in sectors in which such disruption may have cross-border impact.

**Section 17. Provider of Important Services**

* (1) Within the meaning of this Law, a provider of important services is a person which is not a provider of essential services and which is:

1) a medium performer of economic activity which performs economic activity in at least one of the fields referred to in Section 16, Paragraph one, Clause 8 of this Law;

2) a medium or large performer of economic activity which is:

a) a postal operator;

b) a waste manager;

c) a manufacturer or distributor of chemical substances or their mixtures;

d) a merchant which manufactures articles from chemical substances or their mixtures;

e) a food establishment and a food supply logistics undertaking;

f) a manufacturer of medical devices;

g) a manufacturer of computers, electronic and optical products;

h) a manufacturer of electrical equipment;

i) a manufacturer of devices, machinery, and equipment not elsewhere classified;

j) a manufacturer of motor vehicles, trailers, and semi-trailers;

k) a manufacturer of other transport equipment;

l) a provider of online marketplace services;

m) a provider of online search engine services;

n) a provider of social networking services platforms;

o) a scientific institution;

p) a provider of security guard services;

3) a performer of economic activity which performs economic activity in at least one of the fields referred to in Paragraph one, Clause 2 of this Section and is the only provider of such service in the Republic of Latvia;

4) an institution of indirect administration which provides services or operates in the field governed by private law in at least one of the fields referred to in Paragraph one, Clause 2 of this Section;

5) a maintainer of the education information system;

6) a trust service provider which is not a qualified trust service provider.

* (2) Within the meaning of this Law, an education information system is an information system in which electronic data processing of educatees of an educational institution accredited in the Republic of Latvia is carried out.

**Section 18. Recording of Providers of Essential and Important Services**

* (1) A person shall perform self-assessment, determining its conformity with the status of a provider of essential services or provider of important services. In case of conformity, the person shall, not later than within a month, notify the National Cybersecurity Centre thereof. The following shall be indicated in the notification:

1) the name of the person (in case of a natural person – the given name, surname, and personal identity number), legal status, and form of economic activity, registration number, legal address, and other contact details (for example, official electronic address, electronic mail address, telephone number, website address);

2) information on the field of activity of the person in accordance with the provisions of Sections 16 and 17 of this Law;

3) a list and detailed description of essential and important services provided by the person;

4) the Internet Protocol (IP) address ranges used by the person;

5) the countries where the person provides services;

6) the data of the contact person of the person (given name, surname, office held, telephone number, electronic mail address).

* (2) A provider of essential services and a provider of important services shall, without delay but not later than within two weeks, notify the National Cybersecurity Centre of any changes in the information indicated in the notification referred to in Paragraph one of this Section.
* (3) The National Cybersecurity Centre shall, without undue delay, forward the notifications referred to in Paragraphs one and two of this Section to the European Union Agency for Cybersecurity, excluding the information referred to in Paragraph one, Clause 4 of this Section and other information the disclosure of which is in contradiction with the interests of national security.
* (4) The National Cybersecurity Centre shall compile and the Supervisory Committee of Digital Security shall approve the list of essential and important services and also the list of domain name registration service providers. The list of providers of essential and important providers shall be restricted access information.
* (5) If the person has not notified the National Cybersecurity Centre of its conformity with the status of a provider of essential or important services within the time period specified in this Law, but the information at the disposal of the National Cybersecurity Centre is sufficient to determine the conformity of the abovementioned person with the status of a provider of essential or important services, the Supervisory Committee of Digital Security shall, upon proposal of the National Cybersecurity Centre, include the abovementioned persons in the list of providers of essential and important services, notifying the abovementioned provider of essential or important services thereof in writing. In such case, the provider of essential or important services has the obligation, without delay but not later than within a month from the moment of notification, to notify the information referred to in Paragraph one of this Section to the National Cybersecurity Centre.
* (6) The lists referred to in Paragraph four of this Section shall be reviewed at least once in two years. The National Cybersecurity Centre shall ensure the submission of compiled information on the number, fields of activity, and provided services of providers of essential and important services to the European Commission, the NIS Cooperation Group, and also, upon request, other competent authorities of the European Union.
* (7) The National Cybersecurity Centre may, upon request of the European Commission or another competent authority of the European Union, provide relevant information thereto on the identity of the provider of essential or important services (for example, name, legal status, form of economic activity, contact details, etc. of the provider of essential or important services) unless the disclosure of such information is in contradiction with the interests of national security.

**Section 19. Critical Infrastructure of Information and Communication Technologies**

* (1) Within the meaning of this Law, the critical infrastructure of information and communication technologies is the critical infrastructure of information and communication technologies included in the aggregate of the critical infrastructure approved by the Cabinet.
* (2) The security requirements for the critical infrastructure of information and communication technologies, the measures and the procedures for the planning and implementation thereof shall be determined by the Cabinet.
* (3) The requirements referred to in Paragraph two of this Section for the critical infrastructure of information and communication technologies shall not be lower than the requirements laid down for the providers of essential services in this Law.

**Chapter IV**

**Cybersecurity Management of the Subjects**

**Section 20. Competence of the Head and the Cybersecurity Manager of the Subject**

* (1) Cybersecurity management of the subject shall be ensured by and be the responsibility of the head of the subject. The head of each subject shall determine the responsible person who implements and monitors the implementation of cybersecurity measures in the relevant subject (hereinafter – the cybersecurity manager). The Cabinet shall determine the requirements brought forward for the cybersecurity manager.
* (2) The subject shall, without delay but not later than within five working days after determination of the cybersecurity manager, notify the National Cybersecurity Centre and the Constitution Protection Bureau of determination of the cybersecurity manager. The given name, surname, personal identity number, office held, electronic mail address, and telephone number of the cybersecurity manager shall be indicated in the notification.
* (3) The owner or legal possessor of the critical infrastructure of information and communication technologies shall determine the cybersecurity manager after agreement with the Constitution Protection Bureau which performs inspection of the conformity of the cybersecurity manager with the requirements brought forward.
* (4) The subject shall, without delay but not later than within five working days, notify the National Cybersecurity Centre and the Constitution Protection Bureau of any changes in the information indicated in the notification referred to in Paragraph two of this Section.
* (5) The cybersecurity manager has the following obligations:

1) to organise the security measures of the infrastructure of information and communication technologies of the authority;

2) not less than once a year to perform examination of the security of information and communication technologies and, according to the results thereof, to organise elimination of the deficiencies detected;

3) at least once a year to attend training organised by the computer security incident response team in issues of cybersecurity;

4) not less than once a year to brief the persons employed in the authority on the current cyber risks and cybersecurity.

**Section 21. Minimum Cybersecurity Requirements**

* The Cabinet shall determine the minimum cybersecurity requirements for the subjects and the procedures by which the subjects ensure the conformity of their information and communication technologies with the minimum cybersecurity requirements, and also the requirements and measures to be taken for ensuring the confidentiality, integrity, and availability of electronic communications networks and information systems of the subjects and for data repair.

**Section 22. Obligations of the Subject in the Field of Cyber Threat Management**

* The subject shall take appropriate and commensurate technical, operational, and organisational measures to manage cyber risks for the security of electronic communications networks and information systems used by the subject and to prevent or reduce to the minimum extent possible the impact of cyber incidents on recipients of services of the subjects and on other services.

**Section 23. Plan for the Management of Cyber Risks and the Continuity of Operation**

* (1) The subject has the obligation to develop the plan for the management of cyber risks and the continuity of operation and to ensure regular training to employees for efficient implementation of the measures included in the plan.
* (2) The Cabinet shall determine the type and amount of information to be mandatorily included in the plan for the management of cyber risks and the continuity of operation of the subject and also the procedures for the supervision and control of execution of the plan.

**Section 24. Early Warning Sensors**

* The Cabinet shall determine the criteria for the mandatory installation of cybersecurity early warning sensors in the infrastructure of information and communication technologies of the subject and also the provisions for the installation and use of early warning sensors.

**Section 25. Cybersecurity of Data Centres**

* (1) The subject shall maintain the information systems in its ownership and possession in the infrastructure of information and communication technologies conforming to the minimum cybersecurity requirements or in data centres conforming to the requirements stipulated by the Cabinet (hereinafter – the data centres).
* (2) The Cabinet shall determine:

1) the security requirements for the data centres, the procedures for the conformity evaluation, registration, and supervision of the data centres, and also the obligations of the maintainer of a data centre;

2) the provisions for the deployment of the systems of information and communication technologies in the data centres;

3) the provisions for the establishment and operation of security operations centres in the data centres.

* (3) A security operations centre shall be established and the operation in a data centre shall be ensured by the competent computer security incident response team. The computer security incident response team has the right, within the scope of the security operations centre, to collect, store, and electronically process the data necessary for the identification of cyber threats, including log files, data flows, server performance data. The operator of the data centre, if it has the necessary data at its disposal, may transfer the data obtained using its tools to a competent computer security incident response team.

**Section 26. Protection Against Denial of Service Cyberattack**

* The Cabinet shall determine:

1) the requirements for the protection of the infrastructure and internet resources of information and communication technologies against denial of service cyberattacks;

2) the criteria according to which the infrastructure and internet resources of information and communication technologies shall be included in the list of resources to be protected against denial of service cyberattacks;

3) the procedures by which the conformity of the infrastructure and internet resources of information and communication technologies with the criteria referred to in Clause 2 of this Section are assessed;

4) the procedures for the approval of the list of resources to be protected against denial of service cyberattacks.

**Section 27. Unified National Internet Exchange Point**

* (1) A unified national internet exchange point shall be established and maintained with the purpose of:

1) continuously ensuring the presence of the critical data flow in the territory of the Republic of Latvia only;

2) ensuring the reachability of the information systems necessary for the implementation of important public functions and also for ensuring human health, protection, safety, economic and social welfare in case if global network is not available in the Republic of Latvia;

3) ensuring full operation of the internet and exchange of data flows in the territory of the Republic of Latvia in case of disconnection from the global network.

* (2) A State or local government authority or subject the inclusion of which in the list of recipients of services of a unified national internet exchange point has been supported by the interinstitutional commission is entitled to receive the services of the unified national internet exchange point. The Cabinet shall determine the composition of the commission, the procedures for the establishment and operation thereof.
* (3) The Cabinet shall determine:

1) the procedures for the operation of a unified national internet exchange point and the provision and receipt of services;

2) the criteria for the inclusion of the State and local government authorities and subjects in the list of recipients of services of a unified national internet exchange point;

3) the State and local government authorities and subjects for which the requirement to direct data flow directly through a unified national internet exchange point has been laid down.

**Section 28. Cyber Hygiene Requirements**

* The Cabinet shall determine the basic elements and requirements for cyber hygiene and cyber resilience measures for the implementation of cyber hygiene and cyber resilience measures for the State and local government authorities, derived public entities, and other State authorities, legal persons governed by private law which are fulfilling a task delegated by the State administration, except for State security institutions.

**Chapter V**

**Action in Case of a Cyber Incident**

**Section 29. Action of the Subject in Case of a Cyber Accident**

* (1) In detecting a cyber incident, the subject shall, without delay, carry out all activities necessary for the elimination of the cyber incident and also immediately inform the competent computer security incident response team of the cyber incident and carry out the instructions provided thereby regarding action in case of a cyber incident. In case of a cyber incident, the owner or legal possessor of the critical infrastructure of information and communication technologies shall, without delay, also inform the competent State security institution thereof.
* (2) In case of a significant cyber incident, the subject shall, without undue delay but not later than within 24 hours, submit electronically an early warning regarding the significant cyber incident to the competent computer security incident response team.
* (3) In case of a significant cyber incident, the subject shall, without undue delay but not later than within 72 hours (the trust service provider – within 24 hours), submit electronically the initial report on the significant cyber incident to the competent computer security incident response team.
* (4) In case of a significant cyber incident or cyber threat, the subject shall, without undue delay, inform the recipients of its services, including users of the electronic communications network or information system which might be affected by such significant cyber incident or cyber threat, of the possible cybersecurity measures or means which may be used by the recipients of services to prevent the cyber incident or to mitigate the cyber threat. In the relevant case, the subject, in agreement with the competent computer security incident response team (the owner or legal possessor of the critical infrastructure of information and communication technologies – also with the competent State security institution), shall, without undue delay, inform the recipients of its services also of a significant cyber incident or cyber threat unless the disclosure of such information causes the risk of a new significant cyber incident or otherwise is in contradiction with the interests of national security.
* (5) The subject shall, within a month after submission of the report referred to in Paragraph three of this Section, submit a final report on handling of the significant cyber incident to the competent computer security incident response team. Upon request of the competent computer security incident response team, the subject shall also submit an interim report on handling of the significant cyber incident thereto.
* (6) If it is not possible to handle the significant cyber incident within the time period specified in Paragraph five of this Section, the subject shall submit a progress report on handling of the significant cyber incident to the competent computer security incident response team, meanwhile the final report referred to in Paragraph five of this Section shall be submitted after handling of the significant cyber incident.
* (7) The Cabinet shall determine the content of the warning referred to in Paragraph two of this Section and also of the reports referred to in Paragraphs three, five, and six of this Section and the procedures for informing.
* (8) In case of a cyber incident, the persons to whom the obligations specified in Paragraph one of this Section are not applicable shall perform all activities necessary for the prevention thereof and may, upon their own initiative, inform the competent computer security incident response team of the detected cyber incident. The computer security incident response team shall agree with the person who has notified of the cyber incident on provision of support in the cyber incident handling. Voluntary notification of a cyber incident shall not impose additional obligations on the abovementioned person.
* (9) The subjects and other persons may, upon their own initiative, voluntarily notify the competent computer security incident response team of a near miss or cyber threat. Voluntary notification of a near miss or cyber threat shall not impose additional obligations on the person.
* (10) Upon request of the competent computer security incident response team or the National Cybersecurity Centre, the subject shall close access for the user to the electronic communications network for not longer than five days if the user significantly endangers the rights of other users or security of the electronic communications network, information system, or service. The cyber threat, the duration of the access restriction, and, if necessary, other additional activities to be carried out for the subject (for example, rerouting of the data flow to the infrastructure of the competent computer security incident response team) shall be indicated in the request. Contesting or appealing of the request shall not suspend the operation thereof. The Cabinet shall determine the conditions and procedures by which access to the electronic communications network is closed for the user.

**Section 30. Action of a Computer Security Incident Response Team in Case of a Cyber Incident**

* (1) A computer security incident response team shall, without undue delay, inform the National Cybersecurity Centre of receipt of the early warning referred to in Section 29, Paragraph two of this Law or the notification referred to in Section 29, Paragraph three, four, or five of this Law. The computer security incident response team shall also inform the National Cybersecurity Centre of receipt of the notification referred to in Section 29, Paragraphs seven and eight of this Law.
* (2) The computer security incident response team shall, within 24 hours after receipt of the initial information on a significant cyber incident, agree with the person who notified of a significant cyber incident on provision of support in prevention of a significant cyber incident, provide the initial assessment of the cyber incident, and express proposals for the prevention of the cyber incident.
* (3) If the cyber incident detected endangers national security, the computer security incident response team shall inform the National Cybersecurity Centre and State security institutions thereof. The National Cybersecurity Centre shall inform the Minister for Defence and the minister responsible for the sector.
* (4) If the cyber incident detected has a significant impact on an electronic communications network or the continuity of an electronic communications service, the computer security incident response team shall inform the National Cybersecurity Centre and the Constitution Protection Bureau thereof. The National Cybersecurity Centre shall inform the Public Utilities Commission and also may inform the European Union Agency for Cybersecurity and the CSIRT network.
* (5) In case of a cross-border cyber incident, the competent computer security incident response team shall, without undue delay, inform the competent authorities of the affected European Union Member States and the European Union Agency for Cybersecurity.
* (6) If informing of the public of a significant cyber incident or cyber threat may help to prevent or handle a significant cyber incident, to mitigate cyber threat, or is otherwise within the public interests, the National Cybersecurity Centre or the competent computer security incident response team may, upon previous discussion with the subject, inform the public or assign the subject to inform the public unless the disclosure of the abovementioned information is in contradiction with the interests of national security.

**Section 31. Management of Significant Cyber Incidents and Crises**

* (1) The Cabinet shall approve the cyber incident significance criteria.
* (2) The management of significant cyber incidents and crises shall be ensured by the National Cybersecurity Centre in cooperation with computer security incident response teams and State security institutions.
* (3) The objectives, capacities, resources of and procedures for the management of significant cyber incidents and crises shall be determined in the National Plan for the Crisis Management of Cyber Incidents the development and review of which shall be ensured by the National Cybersecurity Centre in cooperation with State security institutions not less than once in four years. The National Plan for the Crisis Management of Cyber Incidents shall be approved by the Cabinet.
* (4) The following shall be included in the National Plan for the Crisis Management of Cyber Incidents:

1) the tasks, obligations, and mutual cooperation mechanism of the National Cybersecurity Centre, computer security incident response teams, and State security institutions;

2) the training activities related to the implementation of the National Plan for the Crisis Management of Cyber Incidents and play-out in training scenarios;

3) the cooperation framework with foreign and international partners;

4) the cooperation framework with the State and local government institutions and also representatives of the private sector who would potentially be subject to the impact of a significant cyber incident;

5) the procedures and the cooperation framework of the competent institutions for efficient management of significant cyber incidents and crises at the level of the European Union.

* (5) The procedures specified in the National Plan for the Crisis Management of Cyber Incidents shall be regularly included in the training and training activities organised by the National Cybersecurity Centre and other competent authorities.
* (6) The National Cybersecurity Centre shall submit information at the European Commission and the European Cyber Crises Liaison Organisation Network on the National Plan for the Crisis Management of Cyber Incidents, except for information which affects the interests of national security.

**Section 32. Restricting Activities in Case of a Cyber Incident**

* (1) If a cyber incident significantly endangers the security of information systems or electronic communications networks and it is not possible to prevent the cyber incident in any other way, the National Cybersecurity Centre is entitled to take the decision:

1) to disconnect or limit access to the top level domain “.lv” name involved in the cyber incident;

2) to limit access to the internet protocol (IP) address involved in the cyber incident;

3) to limit access to the mobile platform application involved in the cyber incident; or

4) to make changes in entries of the Domain Name System.

* (2) The National Cybersecurity Centre shall take the decision referred to in Paragraph one of this Section in accordance with the procedures laid down in the Administrative Procedure Law, indicating a duration of access limitation in the decision which does not exceed five days and, if necessary, other additional activities to be carried out by the maintainer of the top-level domain “.lv” register and the electronic numbering system (for example, rerouting of the data flow to the infrastructure of the competent computer security incident response team).
* (3) Contesting and appeal of the decision of the National Cybersecurity Centre referred to in Paragraph one of this Section shall not suspend the operation and execution thereof.
* (4) The maintainer of the top-level domain “.lv” register and the electronic numbering system and the provider of electronic communications services have the obligation to execute the decision of the National Cybersecurity Centre referred to in Paragraph one of this Section not later than within one working day after notification thereof.
* (5) Prior to taking the decision referred to in Paragraph one of this Section, the National Cybersecurity Centre shall inform the Constitution Protection Bureau.

**Section 33. Attribution of a Cyber Incident**

* The Cabinet shall determine the procedures and criteria by which Latvia shall carry out the attribution of cyber incidents.

**Chapter VI**

**Coordinated Vulnerability Discovery and Prevention**

**Section 34. Coordinated Vulnerability Discovery**

* (1) If a person discovers a vulnerability in the information system or electronic communications network of the subject, it shall, without delay but not later than within five working days, submit a vulnerability discovery report to the competent computer security incident response team.
* (2) The following information shall be included in the vulnerability discovery report:

1) the date and time of detecting the vulnerability (if possible);

2) the information on the information system or electronic communications network in which the vulnerability has been detected;

* + 3) the description of the vulnerability;

4) the methodologies used for detecting the vulnerability or a description of the sequence of activities carried out;

5) the contact details of the submitter of the vulnerability discovery report;

6) other information which is deemed by the submitter of the vulnerability discovery report as necessary for the identification and prevention of the vulnerability detected.

* (3) The competent computer security incident response team shall confirm the receipt of the vulnerability discovery report, check the information included in the report, and inform the submitter of the report of validity of the information included in the report and the result of prevention of the vulnerability.
* (4) If the information provided in the vulnerability discovery report on vulnerability is valid in the assessment of the computer security incident response team, the computer security incident response team shall, without delay, inform the relevant subject thereof.
* (5) Vulnerability discovery may not be used with malicious intent. Information on the vulnerability discovered shall be restricted access information unless a higher level of classification is provided for in laws and regulations. The submitter of the vulnerability discovery report (the person who discovered the vulnerability) and the relevant subject shall be responsible for non-disclosure of the abovementioned information. The competent computer security incident response team shall determine the conditions, procedures, and extent in which the information on the vulnerability discovered may be disclosed.
* (6) The submitter of the vulnerability discovery report is entitled to submit a vulnerability discovery report anonymously or to request the competent computer security incident response team not to disclose the identity of the submitter of the report to the authorities referred to in Section 12, Paragraph four, Clauses 1–4 of this Law. In such case, the competent computer security incident response team has the obligation to ensure confidentiality of identity of the submitter of the report unless the submitter of the report (the person who discovered the vulnerability) complies with the provisions of this Law and the signs of a criminal offence are not present *prima facie*. The abovementioned obligation to ensure confidentiality shall not apply to the authorities referred to in Section 12, Paragraph four, Clauses 5 and 6 of this Law. Anonymous submission of a vulnerability discovery report shall not exempt the submitter of the vulnerability discovery report from the obligation not to disclose information on vulnerability.

**Section 35. Coordinated Vulnerability Prevention**

* (1) The subject shall, within the time period stipulated by the competent computer security incident response team but not later than within 90 days from the moment of receipt of information, carry out the activities necessary for the prevention of a vulnerability and inform the competent computer security incident response team of the course of the vulnerability prevention.
* (2) If, due to objective reasons, it is not possible to prevent a vulnerability within the time period indicated in Paragraph one of this Section, the computer security incident response team may, upon request of the subject, extend the time period for the prevention of the vulnerability but not later than within 180 days from the moment of submitting the vulnerability discovery report, informing the submitter of the vulnerability discovery report thereof.
* (3) The persons to whom the obligations specified in Paragraph one of this Section do not apply may, upon their own initiative, agree with the submitter of the vulnerability discovery report on the time period for the prevention of the vulnerability, informing the competent computer security incident response team of the course of the vulnerability prevention.
* (4) The competent computer security incident response team shall provide support in communication between the submitter of the vulnerability discovery report and the relevant subject if any of the parties expresses such a wish. The competent computer security incident response team shall perform ex post control in relation to the prevention of the vulnerability disclosed and also ensure confidentiality of the submitter of the vulnerability discovery report in accordance with the provisions of Section 34, Paragraph six of this Law.
* (5) If the vulnerability discovered affects several subjects, the competent computer security incident response team shall coordinate the prevention of such vulnerability in cooperation with all abovementioned subjects.
* (6) If the vulnerability discovered may significantly disrupt the provision or receipt of essential or important services in another European Union Member State, the competent computer security incident response team shall cooperate with the computer security incident response teams of this country for the prevention of the abovementioned vulnerability. If the vulnerability discovered affects more than two European Union Member States, the competent computer security incident response team shall cooperate with the computer security incident response teams of these countries, using the CSIRT network.

**Chapter VII**

**Supervision of the Subjects**

**Section 36. Supervision of the Subjects**

* (1) The supervision of the subject shall include control of conformity with the cybersecurity requirements, on-site checks and remote monitoring of information and communication technologies, data and document checks, including in relation to the risk management and the elimination of the deficiencies detected in conformity evaluations, and also security scanning of electronic communications networks and information systems of the subject.
* (2) The Cabinet shall determine the criteria and procedures by which the security scanning referred to in Paragraph one of this Section is performed.

**Section 37. Supervisory Institution**

* Supervision of the subjects shall be performed by:

1) the National Cybersecurity Centre in relation to the providers of essential and important services, except for the critical infrastructure of information and communication technologies;

2) upon request of the Constitution Protection Bureau in relation to the critical infrastructure of information and communication technologies.

**Section 38. Annual Report on Conformity Self-assessment of the Subjects**

* (1) The subject shall, by 1 July of the current year in accordance with the division of supervision of the subjects specified in Section 37 of this Law, submit the annual report on conformity self-assessment (hereinafter – the self-assessment report) to the National Cybersecurity Centre and the Constitution Protection Bureau.
* (2) The form of the self-assessment report and the content and amount of information to be included shall be determined by the Cabinet.

**Section 39. Conformity Audit of the Subjects**

* (1) The National Cybersecurity Centre and the Constitution Protection Bureau are entitled, in accordance with the division of supervision of the subjects specified in Section 37 of this Law, to perform a conformity audit of the subject or to assign the subject to perform an external audit regarding conformity of the subject with the cybersecurity requirements laid down in this Law and stipulated by the Cabinet if there are suspicions or violations of cybersecurity have been detected.
* (2) An external audit shall be performed by an independent cybersecurity auditor who does not have a conflict of interest with the subject and who is registered in the list of cybersecurity auditors approved by the Supervisory Committee of Digital Security. The Cabinet shall determine the requirements to be brought forward for an external cybersecurity auditor and the procedures for the registration of cybersecurity auditors.
* (3) An external audit in the critical infrastructure of information and communication technologies, in addition to that specified in Paragraph two of this Section, shall be performed by a cybersecurity auditor agreed upon with the Constitution Protection Bureau.
* (4) Costs of the external audit shall be covered by the relevant subject and the violations detected in the audit shall be eliminated by the relevant subject.
* (5) After the end of the external audit, the subject shall, without undue delay, submit a copy of the external audit report to the National Cybersecurity Centre (the owner or legal possessor of the critical infrastructure of information and communication technologies – to the Constitution Protection Bureau). Upon request of the National Cybersecurity Centre or the Constitution Protection Bureau, the subject shall also present evidence which formed the basis for the findings included in the external audit report.

**Section 40. Elimination of Non-conformity of the Subjects**

* (1) In case of detecting non-conformities, the National Cybersecurity Centre and the Constitution Protection Bureau are entitled, in accordance with the division of supervision of the subjects specified in Section 37 of this Law, to express a warning to the subject or to assign the subject:

1) to carry out specific activities for the elimination of a non-conformity, determining a commensurate time period for the elimination of the non-conformity and the procedures for reporting on the course of elimination of the non-conformity;

2) without delay, to discontinue and henceforth preclude action which violates the provisions of this Law;

3) to inform the service recipients or to publish information on the cyber threat, its type and extent, and also the activities necessary for the prevention or mitigation thereof;

4) to inform the service recipients or to publish information on the detected violations of the subject;

5) to suspend the operation of the information system, resource, or e-service of the subject until elimination of the non-conformity detected; or

6) to suspend the trade in the product of information and communication technologies or the provision of the service until elimination of the non-conformity detected.

* (2) If the non-conformity detected causes the risk of a significant cyber incident, the National Cybersecurity Centre and the Constitution Protection Bureau shall inform the Cabinet of the risk detected, but if the non-conformity endangers national security – the National Security Council.
* (3) The subject shall, without undue delay, take all necessary, appropriate, and commensurate measures for the elimination of non-conformities, including carry out the instructions of the National Cybersecurity Centre and the Constitution Protection Bureau.
* (4) The National Cybersecurity Centre and the Constitution Protection Bureau are entitled to perform on-site checks, including to appoint officials for monitoring how the subject fulfils the obligations specified in this Law within a specific time period.

**Section 41. Compulsory Execution of a Legal Obligation**

* (1) If a legal obligation is not executed, the National Cybersecurity Centre may perform compulsory execution of the legal obligation with the aid of a pecuniary penalty in accordance with the procedures laid down in the Administrative Procedure Law insofar as other procedures are not laid down in this Law. Pecuniary penalty may be imposed repeatedly until execution of the legal obligation.
* (2) Before commencement of compulsory execution of the legal obligation, the National Cybersecurity Centre may determine a time period for the subject for voluntary execution of the legal obligation.
* (3) The National Cybersecurity Centre and the Constitution Protection Bureau shall perform compulsory execution of the legal obligation in relation to the critical infrastructure of information and communication technologies upon a motivated request of the Constitution Protection Bureau.
* (4) Before issuing an execution order, the National Cybersecurity Centre shall notify the addressee in writing that the information necessary for issuing an execution order has been obtained. The addressee may, within seven days after receipt of the abovementioned notification, become acquainted with the case, express its opinion, and submit additional information.
* (5) The maximum amount of the pecuniary penalty for a legal person shall be:

1) EUR 10 million or 2 per cent of the total net turnover of the last financial year of the legal person in the world (depending on which sum is larger) if the legal person is the provider of essential services or the owner or legal possessor of the critical infrastructure of information and communication technologies;

2) EUR 7 million or 1.4 per cent of the total net turnover of the last financial year of the legal person in the world (depending on which sum is larger) if the legal person is the provider of important services.

* (6) A pecuniary penalty shall not be imposed on the subject if a fine has already been imposed on the subject for non-execution of this very legal obligation in accordance with Article 58(2)(i) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

**Chapter VIII**

**Other Provisions**

**Section 42. National Cybersecurity Strategy**

* (1) The National Cybersecurity Strategy shall be developed once every four years by the National Cybersecurity Centre in cooperation with State administration institutions, State security institutions, and representatives of the private sector and it shall be approved by the Cabinet.
* (2) The following shall be determined in the National Cybersecurity Strategy:

1) the strategic objectives and model of cybersecurity management, the resources necessary for cybersecurity management;

2) the division of roles of the State administration institutions involved in cybersecurity management and also the national and international cooperative mechanisms;

3) the procedures for the determination of the information and communication technologies and resources to be protected at the national level and for the assessment of cyber risks;

4) the procedures and requirements for the development of cyber incident readiness, response, prevention, and recovery plans, the ways of exchange of information, and also cooperation between the public and private sectors;

5) an aggregate of measures for the improvement of the digital and cybersecurity skills of the public.

* (3) The National Cybersecurity Strategy shall apply to the subjects unless it has been specified otherwise in the Strategy.
* (4) The National Cybersecurity Centre shall, within six months from approval of the National Cybersecurity Strategy, develop and the Cabinet shall approve a plan of measures for achieving the objectives brought forward in the Strategy, identifying the work tasks, the responsible authorities, and the time periods for the fulfilment of the tasks, and the results to be achieved. At least the following measures shall be included in the plan:

1) the measures for promoting security of the supply chains of products and services of information and communication technologies of the subjects;

2) the cybersecurity measures in procurements of products and services of information and communication technologies of State institutions of direct and indirect administration, derived public entities, and other authorities, including in relation to the certification, encryption of information and communication technologies and the use of open source solutions;

3) the measures for the management of vulnerabilities, including for ensuring a coordinated process of vulnerability disclosure and prevention;

4) the measures for ensuring confidentiality, integrity, and availability of the public core of the open internet, including in relation to the cybersecurity of undersea communications cables;

5) to implement the cyber risk management measures;

6) the measures for the promotion of cyber resilience of the subjects and other authorities of the State and private sectors, including small and medium performers of economic activity, and the whole public, the promotion of cybersecurity skills and understanding, the development of cybersecurity education and training programmes, and also ensuring the basic level of cyber hygiene;

7) the measures for the support to cybersecurity research and development initiatives, including the development of cybersecurity tools and the development, improvement, and introduction of a secure infrastructure of information and communication technologies;

8) the measures for the promotion of voluntary exchange of cybersecurity information among the subjects;

9) the measures for active cyber protection.

* (5) The National Cybersecurity Centre shall, twice a year, inform the National Cybersecurity Council of the status of introduction of the National Cybersecurity Strategy.
* (6) The National Cybersecurity Centre shall, within three months after adoption of the National Cybersecurity Strategy, notify the European Commission thereof, excluding information of significance to national security.

**Section 43. Processing of Personal Data**

* (1) In fulfilling the tasks specified in this Law and implementing its rights, a computer security incident response team shall receive and process information identifying a person in order to justify or exclude suspicions of a cyber threat or to prevent it and also to ensure communication with the parties involved.
* (2) A computer security incident response team is entitled to store and analyse data which have been obtained in order to justify or exclude suspicions of a vulnerability and cyber incident and which contain personal data after handling of the vulnerability and cyber incident if it is useful for the disclosure or prevention of related vulnerabilities and cyber incidents.
* (3) A computer security incident response team may transfer personal data to the authorities referred to in Section 10, Paragraph one, Clauses 5 and 6 of this Law in order to recognise and prevent such cyber threat, vulnerability, or cyber incident which might cause or causes threats to national security.
* (4) Computer security incident response teams may transfer personal data to the National Guard to the extent and in the manner that allow to recognise and prevent such cyber threat, vulnerability, or cyber incident which might cause or causes threats to national security if the National Guard is involved in the provision of support to the competent computer security incident response team in accordance with the provisions of the National Guard of the Republic of Latvia Law.
* (5) In fulfilling the tasks specified in this Law and implementing its rights, the Constitution Protection Bureau shall receive, process, store, and analyse data which have been obtained in order to justify or exclude suspicions of a cyber threat, vulnerability, or cyber incident which may cause or causes threats to national security.
* (6) Computer security incident response teams may transfer personal data to the Constitution Protection Bureau to the extent and in the manner in order to recognise and prevent such cyber threat, vulnerability, or cyber incident which might cause or causes threats to national security.

**Transitional Provisions**

* 1. With the coming into force of this Law, the Law on the Security of Information Technologies (*Latvijas Vēstnesis*, 2010, No. 178; 2012, No. 179; 2013, No. 228; 2015, No. 34; 2017, No. 132; 2018, No. 210) is repealed.
* 2. The Cabinet shall, by 1 October 2023, issue Cabinet Regulations “Amendment to Cabinet Regulation No. 236 of 29 April 2003, By-laws of the Ministry of Defence”.
* 3. The Cabinet shall, by 1 January 2024, issue the Cabinet regulations referred to in Section 15, Paragraph two, Section 19, Paragraph two, Section 20, Paragraph one, Section 21, Section 22, Paragraph three, Section 23, Paragraph two, Section 24, Section 25, Paragraph two, Section 26, Section 29, Paragraph seven, Section 38, Paragraph two, and Section 39, Paragraph two of this Law.
* 4. The Cabinet shall, by 1 April 2024, issue the Cabinet regulations referred to in Section 9, Paragraph four, Section 27, Paragraph three, and Section 28 of this Law.
* 5. The Cabinet shall, by 1 October 2024, issue the Cabinet instruction referred to in Section 33 of this Law.
* 6. Until issuing of the regulations referred to in Section 15, Paragraph two of this Law but not longer than until 1 January 2024, Cabinet Regulation No. 695 of 1 November 2016, By-laws of the Supervisory Committee of Digital Security, shall be applicable insofar as it is not in contradiction with this Law.
* 7. Until issuing of the regulations referred to in Section 19, Paragraph two of this Law but not longer than until 1 January 2024, Cabinet Regulation No. 100 of 1 February 2011, Procedures for the Planning and Implementation of Security Measures for the Critical Infrastructure of Information Technologies, shall be applicable insofar as it is not in contradiction with this Law.
* 8. Until issuing of the regulations referred to in Section 20, Paragraph one, Section 21, Section 22, Paragraph three, Section 23, Paragraph two, Section 29, Paragraph seven, Section 38, Paragraph two, and Section 39, Paragraph two of this Law but not longer than until 1 January 2024, Cabinet Regulation of 28 July 2015, Procedures for Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements, shall be applicable insofar as it is not in contradiction with this Law.
* 9. In performing an initial self-assessment in accordance with Section 18, Paragraph one of this Law, a person shall notify the National Cybersecurity Centre of its conformity with the status of the provider of essential or important services not later than within six months after coming into force of this Law. If conformity with the status of the provider of essential or important services has set in after the abovementioned time period, the person shall notify the National Cybersecurity Centre thereof within the time period specified in Section 18, Paragraph one of this Law.
* 10. The list of providers of essential and important services referred to in Section 18, Paragraph four of this Law shall be approved within one year after the day of coming into force of this Law.
* 11. The provisions of Section 20, Paragraph two and Section 29, Paragraphs two, three, four, and five of this Law shall be applied from 1 April 2024.
* 12. The provisions of Section 38, Paragraph one of this Law shall be applied from 1 July 2024.

**Informative Reference to European Union Directives**

* The Law contains legal norms arising from:

1) Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Text with EEA relevance);

2) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 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 (Text with EEA relevance);

3) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code;

4) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

The Law shall come into force on 1 July 2023.

|  |  |  |
| --- | --- | --- |
| The Minister | (signature\*) | G.n. Surname |

\* The document has been signed with secure electronic signature