LIKUMI

Issuer: *Saeima*
Type: law
Adoption: 20.06.2024.
Entry into force: 01.09.2024.

Publication:
Latvijas Vēstnesis, 128A, 04.07.2024.
OP number: 2024/128A.1

The *Saeima*[1] has adopted and
the President has proclaimed the following law:

National Cybersecurity Law

Chapter I
General Provisions

Section 1. Terms Used in the Law

The following terms are used in the Law:

1) **maintainer of the top-level domain name registry** - the authority to which a specific top-level domain has been delegated and which is responsible for the management of such top-level domain, including the registration of domain names in such top-level domain and the technical operation of the top-level domain, and also the operation of its name servers, the maintenance of databases, and the distribution of top-level domain zone files between name servers, regardless of whether any of such activities are performed by the authority itself, except for the use of top-level domain names solely for its own purposes, or by an outsourcing service provider;

2) **data centre** - a premise or a group of premises dedicated to the centralised deployment, interconnection, and operation of information technology and network equipment and providing data storage, processing, and forwarding (transport) services and also all the equipment and infrastructure necessary for the distribution of electricity and climate control;

3) **domain name registration service provider** - a registrar or an authorised person acting on behalf of the registrar, for example, a privacy or proxy registration service provider or reseller;

4) **domain name system** - a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach the respective services and resources;

5) **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;

6) **vulnerability** - a weakness, susceptibility to technical problems, or flaw of information and communication technologies or their services which can be exploited by a cyber threat;

7) **information and communication technologies** - technologies which electronically process information, including create, modify, delete, store, display, forward, or transmit it (hereinafter - the electronic processing), for the fulfilment of their intended tasks with the help of technical aids and ensure communication between technology users;

8) **internet exchange point** - a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;

9) **cyber threat** - any potential circumstance, event, or action corresponding to the definition laid down 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);

10) **cybersecurity** - activities corresponding to the definition laid down in Article 2(1) of Regulation 2019/881;

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

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

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

14) **cyber risk** - the potential for loss or disruption of services caused by the cyber incident which is to be expressed as a combination of the magnitude of such loss or disruption and the likelihood of occurrence of the incident;

15) **cyberattack** - an active act by an attacker for the purpose of disrupting the confidentiality, integrity, or availability of data and services of information and communication technologies;

16) **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 exceeds EUR 50 million and the annual balance sheet total exceeds EUR 43 million;

17) **National Cybersecurity Strategy** - a strategic planning document which lays down the basic principles for the making of cybersecurity policy, the objective and strategic priorities thereof;

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

19) **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 determined by the Cabinet;

20) **denial of service cyberattack** - an attack made against the infrastructure of the service provider for the purpose of disrupting the availability of the service;

21) **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;

22) **network and information system**:

a) an electronic communications network;

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

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

23) **security of network and information systems** - the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the confidentiality, integrity, and availability of the data to be processed electronically or of the services offered by, or accessible via, such network and information systems;

24) **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;

25) **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:

1) the performer of economic activity employs at least 249 employees;

2) the total net turnover of the last financial year of the performer of economic activity is at least EUR 10 million, but does not exceed EUR 50 million, or the annual balance sheet total thereof is at least EUR 10 million, but does not exceed EUR 43 million;

26) **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.

Section 2. Purpose of the Law

The purpose of the Law is:

1) to improve the security of information and communication technologies, including by laying down requirements for the provision and receipt of essential services 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, frameworks of cooperation, and tasks for the promotion of cybersecurity;

3) to promote the implementation of cybersecurity measures so that a cyber threat could be anticipated, prevented and also overcome and its consequences could be liquidated in a timely manner, ensuring, as far as possible, the continuity of the confidentiality, integrity, and availability of services.

Section 3. Scope of Application of the Law

(1) The Law shall apply to:

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

2) the institutions of direct and indirect administration, derived public entities, and other State authorities and also legal persons governed by private law which are fulfilling a task delegated by the public administration (hereinafter all together - 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 such 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) which, in accordance with Section 20 of this Law, are the providers of essential services insofar as Regulation 2022/2554 or other legal acts do not provide for other requirements in matters of cybersecurity requirements for financial entities, cyber threat and risk management (including the management of risks of third-party service providers), operational resilience and continuity, determination of the persons responsible for cybersecurity management, testing, action to be taken in case of a cyber incident, incident reports, and supervision of subjects.

(4) If the legal acts of the European Union governing the specific sector provide for the providers of essential services or important services the obligation to take cybersecurity risk management measures or 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 provisions of this Law, including for the supervision of subjects, shall not be applied to these subjects. If the legal acts of the European Union governing the specific sector do not apply to all providers of essential services and 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 important services to which the abovementioned legal acts of the European Union 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 they conform to at least one of the following features:

1) in terms of impact, the cybersecurity risk management measures are at least equivalent to the requirements laid down in Sections 26, 27, and 28 of this Law;

2) the legal act of the European Union governing the specific sector 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 13 of this Law, and the national competent authority specified in Section 4, Paragraph one of this Law to reports on cyber incidents and, in terms of impact, the requirements for reporting on cyber incidents are at least equivalent to the requirements laid down in Section 34 of this Law.

(6) The Law does not apply to such providers of essential services and important services which conform to all of the following conditions:

1) the service provider is registered in a European Union Member State;

2) the service provider provides in the Republic of Latvia the essential services referred to in Section 20, Clauses 1, 2 and Clause 8, Sub-clauses "s", "t", "u", and "v" of this Law or the essential services referred to in Section 21, Paragraph one, Clause 2, Sub-clauses "l", "m", and "n" of this Law;

3) the service provider does not provide in the Republic of Latvia the essential services or important services that have not been specified in Clause 2 of this Paragraph;

4) the service provider is not the owner or lawful possessor of the critical infrastructure of information and communication technologies;

5) the principal place of establishment of the service provider in the European Union is not the Republic of Latvia.

(7) The Law does not apply to such providers of essential services and important services which are not established in the European Union and the principal place of establishment of the representative whereof in the European Union is not the Republic of Latvia.

(8) Within the meaning of this Law, the principal place of establishment shall be:

1) the European Union Member State in which the decisions in relation to the cybersecurity risk management measures of the service provider are primarily taken;

2) if the country referred to in Clause 1 of this Paragraph cannot be determined - the European Union Member State in which cybersecurity operations are carried out in relation to the service provider;

3) if the country referred to in Clause 2 of this Paragraph cannot be determined - the European Union Member State in which the respective service provider has the highest number of employees within the European Union.

(9) Paragraph eight of this Section does not apply to the cases where the National Cybersecurity Centre, upon request of the competent authority of another European Union Member State, implements the supervision and enforcement measures provided for in this Law in respect of a provider of essential services established in the respective European Union Member State which provides services in the Republic of Latvia or has a network or information system that is located in the Republic of Latvia under its possession.

(10) The Law does not apply to electronic communications merchants which do not provide an electronic communications network and electronic communications services in the Republic of Latvia.

(11) The Law does not apply to such providers of essential services and important services which are public authorities of another European Union Member State.

Chapter II
Authorities Responsible for Cybersecurity

Section 4. National Cybersecurity Centre

The National Cybersecurity Centre is the national competent authority which operates within the Ministry of Defence as the single point of contact in cybersecurity matters and implements national cybersecurity supervision, forms initiatives of the national cybersecurity action policy, and, within the limits of the competence thereof, forms and implements international cooperation.

Section 5. Tasks of the National Cybersecurity Centre

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

1) to coordinate cooperation in cybersecurity matters with the competent authorities 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;

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

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

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

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

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

9) to ensure the operation of the unified national internet exchange point and also to coordinate the 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 National Plan for Cyber Incident Crisis Management 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 the providers of essential services 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;

13) to cooperate with the competent authorities of other European Union Member States, including to send them the information received 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 Network and Information Systems Cooperation Group of the European Union (hereinafter - the NIS Cooperation Group) and to implement the related tasks;

16) to exercise 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 conforming to the requirements stipulated by the Cabinet;

20) to participate in coordinated vulnerability discovery and prevention within the limits of its competence;

21) if 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) if necessary, to participate in assessments of the cybersecurity capacity and action policy of the 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 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, 18, 19, 20, 21, 22, and 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

The National Cybersecurity Centre shall have the following rights:

1) to request and receive information from the providers of essential services and important services on the

information and communication technologies in their ownership and possession, on the cybersecurity and cyber risk management measures implemented and planned thereby and also on cyber incidents, near misses, cyber threats, and vulnerabilities;

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

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

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

5) to impose a fine and to perform the compulsory enforcement of a legal obligation;

6) to request and receive from the operators of data centres information on the fulfilment of the obligations imposed thereon.

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 imposed thereon by this Law;

2) to cooperate with the owners and legal possessors of the critical infrastructure of information and communication technologies for the 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 legal acts.

Section 8. Rights of the Constitution Protection Bureau

The Constitution Protection Bureau shall have the following rights:

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

2) to provide instructions to ensure the fulfilment of the obligations specified in this Law for the owners and legal possessors of the critical infrastructure of information and communication technologies or to prevent threat to national security;

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

4) to impose a fine and to perform the compulsory enforcement of a legal obligation.

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 the prevention of cyber incidents.

(2) The tasks of computer security incident response teams shall be performed by:

1) the Defence Intelligence and Security Service with regard to the Ministry of Defence, the 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 the authorities 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 exercise the rights in accordance with this Law under functional subordination of the Minister for Defence which is implemented in the form of control.

(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, if necessary, other institutions with the information on current significant cyber incidents, cyber incidents, near misses, cyber threats, and vulnerabilities;

4) to organise educational measures, perform analytical and research work, and organise thematic trainings 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 authorities and computer security incident response teams of the European Union, foreign and international organisations, to participate in the network of computer security incident response teams of the European Union Member States (hereinafter - the CSIRT network);

7) to inform without delay the National Cybersecurity Centre and State security institutions of the significant cyber incident and also to inform the competent authority of another European Union Member State of the significant cyber incident which disrupts the continuity of operation of an essential service 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 reported on a cyber incident;

9) within the limits of its competence, to cooperate with the State and private sector authorities in order to facilitate cybersecurity and cyber resilience, and also 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 the networks and information systems of the subject to detect vulnerabilities with potentially essential impact;

11) to fulfil other obligations imposed thereon by the legal acts.

Section 11. Rights of Computer Security Incident Response Teams

(1) Computer security incident response teams shall have the following rights:

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 threats;

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

3) to perform inspections in the infrastructure of information and communication technologies of the providers of essential services 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 services or important services in

the particular Member State;

6) to carry out proactive target system and network 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 upon agreement with the Constitution Protection Bureau.

Section 12. Decisions and Requests Issued by the National Cybersecurity Centre and the Constitution Protection Bureau and Legal Obligations Imposed Thereby

(1) If the addressee of the decision, request, or legal obligation is a legal person governed by private law, the decision, request, or the legal obligation accordingly issued or imposed by the National Cybersecurity Centre and the Constitution Protection Bureau is an administrative act.

(2) If the addressee of the decision, request, or legal obligation is an institution of direct or indirect administration, another State authority, or a derived public entity, the decision, request, or the legal obligation accordingly issued or imposed by the National Cybersecurity Centre and the Constitution Protection Bureau is not an administrative act.

(3) The Cabinet shall determine the procedures for reporting on the institutions of direct or indirect administration, other State authorities, and derived public entities that fail to comply with the decisions, requests, or the imposed legal obligations referred to in this Law.

(4) The decision, request, and legal obligation referred to in Paragraph two of this Section shall be accordingly issued or imposed in writing and shall include the following information:

1) the name and address of the institution;

2) the addressee;

3) the determination of facts;

4) the justification for the decision, request, or legal obligation;

5) a separate listing of the legal norms applied (indicating also Section of the regulatory enactment, its Paragraph, Clause, or Sub-clause);

6) the rights granted to the addressee and the rights rejected;

7) the conditions (if necessary);

8) the procedures for contesting the decision, request, or legal obligation.

(5) The decision, request, and legal obligation referred to in Paragraphs one and two of this Section may be contested as follows:

1) the decision, request, or the legal obligation accordingly issued or imposed by the National Cybersecurity Centre in respect of the providers of essential services and important services - by submitting a relevant submission to the Minister for Defence. The decision of the Minister for Defence on the contested decision, request, or legal obligation referred to in Paragraph one of this Section may be appealed in accordance with the procedures laid down in the Administrative Procedure Law. The decision of the Minister for Defence on the contested decision, request, or legal obligation referred to in Paragraph two of this Section shall not be subject to appeal;

2) the decision, request, or the legal obligation accordingly issued or imposed by the Constitution Protection Bureau in respect of critical infrastructure of information and communication technologies - by submitting a relevant submission to the Director of the Constitution Protection Bureau. The decision of the Director of the Constitution Protection Bureau on the contested decision, request, or legal obligation referred to in Paragraph one of this Section may be appealed in accordance with the procedures laid down in the Administrative Procedure Law. The decision of the Director of the Constitution Protection Bureau on the contested decision, request, or legal obligation referred to in Paragraph two of this Section shall not be subject to appeal.

Section 13. Cooperation of the Competent Authorities

(1) The National Cybersecurity Centre, the Constitution Protection Bureau, and computer security incident response teams shall, as necessary, 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, but not less

than once in a quarter, mutually exchange information on topicalities in supervision of the subjects, including on 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, the Constitution Protection Bureau, and computer security incident response teams shall, regularly but not less than twice in a year, exchange information on the current cyber incidents and cyber threats with the following authorities, unless exchange of such information is in contradiction with the interests of national security:

1) Latvijas Banka - in matters related to cybersecurity of the financial entities referred to in Article 2 of Regulation 2022/2554, including the provision of such information to Latvijas Banka which is at the disposal thereof in relation to the detected cyber incidents in the information and communication technology infrastructure of the subjects referred to in Section 20, Clause 8, Sub-clause "k" of this Law, and also exchange of information on cyber incidents, current or potential cyber threats that may affect the performance of tasks of Latvijas Banka laid down in the legal acts of the European Union and the laws and regulations of Latvia;

2) the Public Utilities Commission - in matters 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 as the responsible institution in the field of civil aviation security which implements the supervisory functions thereof referred to in Article 9 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 limited liability company Latvian Maritime Administration - in matters related to the implementation and supervision of security requirements for ships, shipping companies, ports, and port facilities;

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

6) the Supervisory Committee of Digital Security - in matters related to electronic identification service providers and the services provided thereby, trusted certification service providers and the services provided thereby, online signature collection systems, and the providers of essential services and important services;

7) the competent authorities of the police, the Office of the Prosecutor, the court, and other competent authorities - in matters related to the prevention, detection, and investigation of criminal offences. 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 authority thereof, providing thereto the information at the disposal thereof which is necessary for the performance of procedural activities;

8) State security institutions - in matters 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 endanger national security.

(4) The Institute of Mathematics and Computer Science of the University of Latvia shall provide the Defence 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.

(5) The Defence Intelligence and Security Service shall provide information to the Institute of Mathematics and Computer Science of the University of Latvia which is necessary for the performance 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.

(6) If the matters referred to in Paragraph three, Clause 1 of this Section are related to the information and communication technology infrastructure maintained by the Eurosystem, Latvijas Banka shall forward the information provided by the competent authority to the European Central Bank.

Section 14. Cooperation of the Competent Authorities with the Competent Authorities of Other European Union Member States

(1) If a provider of essential services or a provider of important services provides services in more than one European Union Member State or provides services in one or more European Union Member States and its network and information systems are located in one or several other European Union Member States, the National

Cybersecurity Centre, the Constitution Protection Bureau, and computer security incident response teams shall, if necessary, cooperate with the competent authorities of other European Union Member States:

1) inform the competent authorities of other relevant European Union Member States through the National Cybersecurity Centre and exchange information on the supervision and enforcement measures taken;

2) if necessary, send a request for information or request the competent authority of another European Union Member State to take supervision and enforcement measures;

3) upon receipt of a justified request for mutual assistance from the competent authority of another European Union Member State, provide assistance to the respective competent authority to ensure that supervision or enforcement measures are taken effectively and consistently.

(2) The mutual assistance referred to in Paragraph one, Clause 3 of this Section may include requests for information and supervision measures, including requests for on-site checks, remote monitoring, or targeted security audits.

(3) The National Cybersecurity Centre, the Constitution Protection Bureau, and computer security incident response teams shall ensure the implementation of the request for mutual assistance, unless it is established that they are not competent to provide the requested assistance, the requested assistance is not proportionate to the supervisory tasks of the competent authorities, or the received request for mutual assistance is in contradiction with the interests of national security.

(4) Prior to rejecting a received request for mutual assistance, the National Cybersecurity Centre, the Constitution Protection Bureau, and computer security incident response teams shall consult with each other. If requested by a European Union Member State, the abovementioned competent authorities shall consult the European Commission and the European Union Agency for Cybersecurity before refusing a request for mutual assistance.

(5) The National Cybersecurity Centre, the Constitution Protection Bureau, and computer security incident response teams may, by common agreement with the competent authority of another European Union Member State, carry out joint supervision of subjects.

Section 15. 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 the National Cybersecurity Centre, the Constitution Protection Bureau, and computer security incident response teams, providing them with the necessary information and meeting the lawful requirements thereof.

Section 16. 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 17. 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, according to the competence thereof, cooperate with the Supervisory Committee of Digital Security and provide to the respective Committee the information necessary for the implementation of the functions thereof, including inform of the detected significant cyber incidents and cyber threats which affect qualified trust service providers or qualified trust services provided thereby.

Section 18. 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 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 the procedures for the 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 therein.

(4) The National Cybersecurity Centre shall, within six months after 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 limit 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 improving the 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 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) the measures for the implementation of the cyber risk management;

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) active cyber protection measures.

(5) The National Cybersecurity Centre shall, twice a year, inform the National Cybersecurity Council of the progress 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, except for the information of significance to national security.

Section 19. Processing of Personal Data

(1) When performing its 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 in order to exclude suspicions of a cyber threat or to prevent it and also to ensure communication with the parties involved.

(2) After handling of the vulnerability and cyber incident, 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 if the abovementioned information 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 9, Paragraph two of this Law in order to recognise and prevent such cyber threat, vulnerability, or cyber incident which causes or might cause threats to national security.

(4) Computer security incident response teams may transfer personal data to the National Guard of the Republic of Latvia to the extent and in the manner necessary to recognise and prevent such cyber threat, vulnerability, or cyber incident which causes or might cause threats to national security if the National Guard of the Republic of Latvia is involved in the provision of support to the competent computer security incident response team in accordance with the

National Guard of the Republic of Latvia Law.

(5) When performing its 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 causes or might cause threats to national security.

(6) A computer security incident response team may transfer personal data to the Constitution Protection Bureau to the extent and in the manner necessary to recognise and prevent such cyber threat, vulnerability, or cyber incident which causes or might cause threats to national security.

Chapter III
Identification and Recording of the Subjects

Section 20. Provider of Essential Services

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

1) a maintainer of the top-level domain name registry, for example, the holder of the top-level domain ".lv" registry;

2) a provider of domain name system services which provides publicly available recursive domain name resolution services for internet end-users or authoritative domain name resolution services for third-party usage, except for root name servers;

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) the public electronic mass 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, an aircraft operator, or an operator of an aerodrome or other civil aviation objects and facilities;

e) a railway undertaking or a railway infrastructure manager;

f) a shipping company, except for individual ships managed by the respective company;

g) a port authority;

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

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

j) 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;

l) a medical treatment institution or a European Union reference laboratory;

m) a merchant which carries out research and development activities in respect of medicinal products, manufactures medicinal products and active substances;

r) a manufacturer of critical medical devices (in accordance with 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 for the case where the principal activity of the merchant is not related to the distribution of drinking water;

p) a water management service provider;

r) an internet exchange point service provider;

s) a cloud computing service provider;

t) a data centre service provider;

u) a content delivery network service provider;

v) 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 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 governed by private law in at least one of the fields referred to in Clause 8 of this Section;

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

Section 21. Provider of Important Services

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

1) a medium performer of economic activity which performs economic activity in at least one of the fields referred to in Section 20, 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 in wholesale trade if distribution of chemical substances or their mixtures is the principal activity of the merchant;

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

e) a merchant the principal activity of which is industrial food production, processing, or wholesale distribution of food;

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 personal data processing of educatees of an educational institution accredited in the Republic of Latvia is carried out.

Section 22. Recording of Providers of Essential Services and Important Services

(1) A person shall perform self-assessment, determining its conformity with the status of the provider of essential services or the 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 (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 Sections 20 and 21 of this Law;

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

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

5) the countries where the person provides services;

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

(2) The providers of essential services and 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 delay, forward the notifications referred to in Paragraphs one and two of this Section to the European Union Agency for Cybersecurity, except for 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 the providers of essential services and important services. The list of the providers of essential services and important services shall be restricted access information.

(5) If the person has not notified the National Cybersecurity Centre of its conformity with the status of the provider of essential services or the provider of important services within the time limit 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 the provider of essential services or the provider of important services, the Supervisory Committee of Digital Security shall, upon proposal of the National Cybersecurity Centre, include the abovementioned person in the list of the providers of essential services and important services, notifying the abovementioned provider of essential services or important services thereof in writing. In such case, the provider of essential services or important services has the obligation, without delay but not later than within a month after receipt of the notification, to provide the information referred to in Paragraph one of this Section to the National Cybersecurity Centre.

(6) The list 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 the 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 information thereto on the identity of the provider of essential services or important services (for example, name, legal status, form of economic activity, contact details, etc. of the provider of essential services or important services) unless the disclosure of such information is in contradiction with the interests of national security.

Section 23. Recording of Domain Name Registration Service Providers and Requirements for a Domain Name Registration Database

(1) A domain name registration service provider which conforms to the status of the domain name registration

service provider and the decisions of which in relation to cybersecurity are taken in the Republic of Latvia or which has the highest number of employees in the Republic of Latvia shall notify the National Cybersecurity Centre thereof not later than within a month. The following shall be indicated in the notification:

1) the name of the person (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 Sections 20 and 21 of this Law, if applicable;

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

4) the countries where the person provides services;

5) the data of the contact person of the person (given name, surname, position, telephone number, electronic mail address).

(2) A domain name registration service provider 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 delay, forward the notifications referred to in Paragraphs one and two of this Section to the European Union Agency for Cybersecurity, except for the information referred to in Paragraph one, Clause 3 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 domain name registration service providers.

(5) If the person has not notified the National Cybersecurity Centre of its conformity with the status of the domain name registration service provider within the time limit 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 the domain name registration service provider, the Supervisory Committee of Digital Security shall, upon proposal of the National Cybersecurity Centre, include the abovementioned person in the list of domain name registration service providers, notifying the abovementioned domain name registration service provider thereof in writing. In such case, the domain name registration service provider has the obligation, without delay but not later than within a month after receipt of the notification, to provide the information referred to in Paragraph one of this Section to the National Cybersecurity Centre.

(6) The requirements for a domain name registration database applicable to the maintainer of the top-level domain ".lv" registry and domain name registration service provider shall be determined by the Cabinet.

Section 24. 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 may 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 25. 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 to be brought forward for the cybersecurity manager.

(2) The subject shall, without delay but not later than within five working days, notify the National Cybersecurity Centre and the Constitution Protection Bureau of determination of the cybersecurity manager. The given name, surname, personal identity number, position, 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 inspects 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 carry out security screening 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 matters of cybersecurity;

4) not less than once a year to ensure the instruction of the persons employed in the authority on the cyber risks and cybersecurity relevant to the subject.

Section 26. Minimum Cybersecurity Requirements

The Cabinet shall determine the minimum cybersecurity requirements for the subjects, the procedures by which the subjects shall ensure the conformity of their networks and information systems with the minimum cybersecurity requirements, the requirements and measures to be taken for ensuring the confidentiality, integrity, and availability of the networks and information systems of the subjects and for data repair, and also the manner in which the information referred to in Section 22, Paragraphs one, two, and five, Section 23, Paragraphs one, two, and five, and Section 25, Paragraphs two and four of this Law shall be provided to the National Cybersecurity Centre and the Constitution Protection Bureau (for example, through the State information system maintained by the National Cybersecurity Centre or another technological solution).

Section 27. Obligations of the Subject in the Field of Cyber Threat Management

The subject shall take appropriate and commensurate technical 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 28. Plan for the Management of Cyber Risks and the Continuity of Operation of Information and Communication Technologies

(1) The subject has the obligation to develop the plan for the management of cyber risks and the continuity of operation of information and communication technologies 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 information and communication technologies of the subject and also the procedures for the supervision and control of execution of the plan.

Section 29. 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 30. Cybersecurity of Data Centres

(1) The subject shall maintain the information systems in its ownership or possession in the infrastructure of information and communication technologies thereof 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 operator of a data centre;

2) the regulations regarding the deployment of information systems in the data centres;

3) the regulations regarding the establishment and operation of security operations centres in the data centres.

(3) The competent computer security incident response team has the right to establish a security operations centre in a data centre of national importance, institutions of direct and indirect administration, derived public entities, and other public authorities and to ensure the operation thereof. 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 shall, if it has the necessary data at its disposal, transfer the data obtained using its tools to a competent computer security incident response team.

(4) The competent computer security incident response team is entitled to establish a security operations centre in the critical infrastructure of information and communication technologies by assessing the capacity of existing and planned security operations centres in the critical infrastructure of information and communication technologies.

Section 31. Centralised Protection against Denial of Service Cyberattack

The Cabinet shall determine:

1) the requirements for the centralised protection of the infrastructure and internet 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 in a centralised manner 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 shall be assessed;

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

Section 32. Operation of a Unified National Internet Exchange Point

(1) A unified national internet exchange point shall be established and maintained for:

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 where global internet 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 internet.

(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 abovementioned 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 33. Cyber Hygiene Requirements

The Cabinet shall determine for the subjects the basic elements and requirements for cyber hygiene measures in respect of the implementation of cyber hygiene measures.

Chapter V
Action to be Taken in Case of a Cyber Incident

Section 34. Action of the Subject in Case of a Cyber Incident

(1) When detecting a cyber incident, the subject, without delay, shall implement all activities necessary for the elimination of the cyber incident and also inform without delay the competent computer security incident response team of the cyber incident and comply with the instructions provided thereby regarding action to be taken 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. The Cabinet shall determine the procedures for the informing of cyber incidents and the criteria for such cyber incidents information on which must be provided to the competent computer security incident response team.

(2) In case of a significant cyber incident, the subject shall, without 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 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 a significant cyber threat, the subject shall, without 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 significant 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, after reaching 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 inform without delay the recipients of its services also of a significant cyber incident or a significant 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 the 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 the handling of the significant cyber incident thereto.

(6) If the significant cyber incident cannot be handled within the time limit specified in Paragraph five of this Section, the subject shall submit a progress report on the 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 submission procedures.

(8) In case of a cyber incident, the persons to whom the obligations specified in Paragraph one of this Section are not applicable may 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 reported on the cyber incident on the 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 National Cybersecurity Centre or the Constitution Protection Bureau, 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 activities to be carried out by 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 shall be closed for the user.

Section 35. Action of a Computer Security Incident Response Team in Case of a Cyber Incident

(1) A computer security incident response team shall, without delay, inform the National Cybersecurity Centre of receipt of the early warning referred to in Section 34, Paragraph two of this Law or the notification referred to in Section 34, Paragraph three, five, or six 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 34, Paragraphs eight and nine 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 reported on a significant cyber incident on provision of support in

prevention of a significant cyber incident, and also 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 thereof 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 thereof 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 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 36. 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 Cyber Incident Crisis Management 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 Cyber Incident Crisis Management shall be approved by the Cabinet.

(4) The following shall be included in the National Plan for Cyber Incident Crisis Management:

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 related to the implementation of the National Plan for Cyber Incident Crisis Management;

3) the framework for cooperation with foreign and international partners;

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

5) the cooperation framework of competent authorities and the procedures for efficient management of significant cyber incidents and crises in the European Union.

(5) The procedures specified in the National Plan for Cyber Incident Crisis Management 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 to the European Commission and in the European Cyber Crises Liaison Organisation Network on the National Plan for Cyber Incident Crisis Management, except for information which affects the interests of national security.

Section 37. Restricting Activities in Case of a Cyber Threat or a Cyber Incident

(1) If a cyber threat or a cyber incident causes or might cause a significant threat to the security of information systems and electronic communications networks or national security and the cyber incident or cyber threat cannot be prevented in any other way, the National Cybersecurity Centre or the Constitution Protection Bureau, by restricting access to internet resources, is entitled to take the decision:

1) to disconnect or limit access to the domain name involved in the cyber incident or cyber threat;

2) to limit access to the Internet Protocol (IP) address involved in the cyber incident or cyber threat;

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

(2) The decision of the National Cybersecurity Centre or the Constitution Protection Bureau referred to in Paragraph

one of this Section shall specify the limitation of access and the duration thereof which shall not exceed one year.

(3) Contesting and appeal of the decision of the National Cybersecurity Centre or the Constitution Protection Bureau referred to in Paragraph one of this Section shall not suspend the operation and enforcement thereof.

(4) The providers of electronic communications services shall comply with the decision of the National Cybersecurity Centre or the Constitution Protection Bureau referred to in Paragraph one, Clauses 2 and 3 of this Section not later than within one working day after notification thereof, provided that the technological means necessary for compliance with the decision are at the disposal thereof.

(5) The providers of electronic communications services and maintainer of the top-level domain name registry shall comply with the decision of the National Cybersecurity Centre or the Constitution Protection Bureau referred to in Paragraph one, Clause 1 of this Section without delay after notification thereof, using the list of restricted internet resources maintained by the competent computer security incident response team and shall restrict access of end-users to the internet resources included in the list, also ensuring without delay that information on end-user attempts to access the restricted resources is forwarded to the competent computer security incident response team.

(6) In accordance with the division of supervision of the subjects specified in Section 41 of this Law, the National Cybersecurity Centre or the Constitution Protection Bureau shall consult Latvijas Banka prior to exercising the rights referred to in Paragraph one, Clauses 1 and 2 of this Section in respect of disabling or restricting access to a domain name registered in the name of Latvijas Banka or restricting access to the Internet Protocol (IP) address of Latvijas Banka.

Section 38. Attribution of Cyberattacks

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

Chapter VI
Coordinated Vulnerability Discovery and Prevention

Section 39. 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 on the vulnerability provided in the vulnerability discovery report has been assessed by the competent computer security incident response team as justified, the competent computer security incident response team shall, without delay, inform the respective subject and the Constitution Protection Bureau, provided that this applies to the critical infrastructure of information and communication technologies.

(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 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 to which the information on the specific 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. 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 complies with the requirements laid down in 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 13, Paragraph three, Clauses 7 and 8 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 40. Coordinated Vulnerability Prevention

(1) The subject shall, within the time limit stipulated by the competent computer security incident response team but not later than within 90 days after receipt of information, take 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 limit specified in Paragraph one of this Section, the computer security incident response team may, upon request of the subject, extend the time limit for the prevention of the vulnerability but for not more than 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 limit for the prevention of the vulnerability and inform 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 of the prevention of the vulnerability disclosed and also ensure confidentiality of the submitter of the vulnerability discovery report in accordance with Section 39, 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 could significantly disrupt the provision or receipt of essential services 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 and Enforcement Measures

Section 41. Supervisory Institutions

Supervision of the subjects shall be performed by:

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

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

Section 42. Supervision of the Subjects

(1) The supervision of the subject shall include control of compliance 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) In accordance with the division of supervision of the subjects specified in Section 41 of this Law, the National Cybersecurity Centre and the Constitution Protection Bureau are entitled to prioritise the implementation of the supervision measures referred to in Paragraph one of this Section by assessing the current cyber risks.

(3) The Cabinet shall determine the criteria and procedures for the performance of the security scanning referred to in Paragraph one of this Section.

Section 43. Report on Conformity Self-assessment of the Subjects

(1) In accordance with the division of supervision of the subjects specified in Section 41 of this Law, the subject shall submit the 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 the information to be included therein and also the time limit and regularity for the submission of the report shall be determined by the Cabinet.

Section 44. Conformity Audit of the Subjects

(1) In accordance with the division of supervision of the subjects specified in Section 41 of this Law, the National Cybersecurity Centre and the Constitution Protection Bureau are entitled 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 regulations if there are suspicions of cybersecurity violations or they have been detected.

(2) An external audit shall be performed by an independent cybersecurity auditor who does not have a conflict of interests 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 a cybersecurity auditor and the procedures for the registration of cybersecurity auditors.

(3) An external audit in the critical infrastructure of information and communication technologies shall be performed by a cybersecurity auditor corresponding to the criteria specified in Paragraph two of this Section agreed upon with the Constitution Protection Bureau.

(4) Costs of the external audit shall be covered by 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 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 conclusions included in the external audit report.

Section 45. 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 41 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 limit for the elimination of the non-conformity and the procedures for reporting on the course of elimination of the non-conformity;

2) to discontinue without delay and henceforth preclude any action which violates the requirements laid down in 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.

(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 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.

(5) If the subject fails to comply with the legal obligations imposed in accordance with Paragraph one of this Section, the National Cybersecurity Centre and the Constitution Protection Bureau are entitled, in accordance with the division of supervision of the subjects specified in Section 41 of this Law:

1) to request the subject to suspend the operation of its information system, resource, or electronic service until

elimination of the non-conformity detected;

2) to request the subject 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;

3) to temporarily prohibit any natural person who is responsible for the fulfilment of management and representation duties in the subject at the level of an executive body or an equivalent level from carrying out management and representation functions.

(6) When deciding on any of the enforcement measures referred to in Paragraph one or three of this Section, the National Cybersecurity Centre and the Constitution Protection Bureau shall take into account the following considerations:

1) the severity of the non-conformity and the significance of the non-conformity, taking into account that the following shall be considered as significant cases of non-conformity within the meaning of this Law:

a) detection of repeated cases of non-conformity;

b) failure to report or resolve significant incidents;

c) failure to eliminate the non-conformity detected, contrary to the instructions provided by the National Cybersecurity Centre and the Constitution Protection Bureau;

d) obstruction of audits or supervisory activities requested by the National Cybersecurity Centre and the Constitution Protection Bureau following detection of the non-conformity;

e) provision of false or inaccurate information in relation to cybersecurity risk management measures or reporting measures;

2) the duration of the non-conformity;

3) any previous cases of non-conformity by the respective subject;

4) any material or non-material damage caused, including any financial or economic loss, the impact on other services, and the number of users affected;

5) the intent or negligence of the person causing the non-conformity;

6) any measures taken by the subject to prevent or minimise material or non-material damage;

7) whether the subject complies with the internal rules issued to fulfil the minimum cybersecurity requirements, the plan for the management of cyber risks and the continuity of operation, and also the international and national standards and certification schemes (if applicable) binding on the subject;

8) the extent to which the natural person responsible for the fulfilment of management and representation duties in the subject at the level of an executive body or an equivalent level cooperates with the National Cybersecurity Centre and the Constitution Protection Bureau.

(7) The National Cybersecurity Centre and the Constitution Protection Bureau shall send the decision referred to in Paragraph five, Clause 3 of this Section to the subject.

(8) The prohibition referred to in Paragraph five, Clause 3 of this Section shall not apply to a provider of important services who is not the owner or legal possessor of critical infrastructure of information and communication technologies.

(9) The prohibition referred to in Paragraph five, Clause 3 of this Section shall apply until the respective subject has fulfilled the legal obligations imposed thereon in accordance with Paragraph one of this Section.

(10) After the subject has fulfilled the legal obligations imposed thereon in accordance with Paragraph one of this Section, the National Cybersecurity Centre and the Constitution Protection Bureau shall, in accordance with the division of supervision of the subjects specified in Section 41 of this Law, cancel the prohibition referred to in Paragraph five, Clause 3 of this Section.

(11) The prohibition referred to in Paragraph five, Clause 3 of this Section shall not apply to institutions of direct and indirect administration, other public authorities, and derived public entities.

(12) In accordance with the division of supervision of the subjects specified in Section 41 of this Law, the National Cybersecurity Centre or the Constitution Protection Bureau shall consult Latvijas Banka prior to exercising the rights referred to in Paragraph five, Clause 1 of this Section in respect of information systems, resources, or electronic services maintained by Latvijas Banka.

Section 46. Imposition of a Fine and Provisions for the Compulsory Enforcement

(1) The National Cybersecurity Centre is entitled to impose a fine of up to EUR 10 million on a provider of essential services for a major non-conformity with the requirements laid down in this Law, but up to two per cent of the total net turnover of the provider of essential services in the last financial year if the total net turnover of the provider of essential services in the last financial year exceeds EUR 500 million.

(2) The National Cybersecurity Centre is entitled to impose a fine of up to EUR 7 million on a provider of important services for a major non-conformity with the requirements laid down in this Law, but up to 1.4 per cent of the total net turnover of the provider of important services in the last financial year if the total net turnover of the provider of important services in the last financial year exceeds EUR 500 million.

(3) The Constitution Protection Bureau is entitled to impose a fine of up to EUR 10 million on the owner or legal possessor of critical infrastructure of information and communication technologies for a major non-conformity with the requirements laid down in this Law, but up to two per cent of the total net turnover of the owner or legal possessor of critical infrastructure of information and communication technologies in the last financial year if the total net turnover of the owner or legal possessor of critical infrastructure of information and communication technologies in the last financial year exceeds EUR 500 million.

(4) The Cabinet shall determine the procedures for the determination of the net turnover of the financial year from which the fine is calculated, and the criteria for the determination of the amount of the fine.

(5) Within the meaning of this Law, a major non-conformity means that:

1) the subject fails to take appropriate and proportionate technical and organisational measures to minimise the impact of a cyber threat or a cyber incident;

2) the subject repeatedly refuses to fulfil the legal obligations imposed by the officials of the National Cybersecurity Centre or the Constitution Protection Bureau related to the obligation of the subject to provide information within the scope of the cyber security supervision imposed by this Law;

3) the subject fails to notify the competent computer security incident response team of a significant cyber incident within the time limit laid down in this Law or knowingly provides false information to the competent computer security incident response team.

(6) The amount of the fine shall be determined in proportion to the violation committed. When taking the decision to impose a fine and deciding on the amount thereof, the National Cybersecurity Centre and the Constitution Protection Bureau shall assess and take into account the considerations referred to in Section 45, Paragraph six of this Law and also the financial situation of the person.

(7) The decision to impose a fine of the National Cybersecurity Centre and the Constitution Protection Bureau may be appealed before a court in accordance with the procedures laid down in the Administrative Procedure Law.

(8) The subject shall pay the fine imposed by the National Cybersecurity Centre or the Constitution Protection Bureau within one month from the date of entry into effect of the decision on the imposition thereof. If the decision to impose a fine has not been complied with voluntarily, compulsory enforcement thereof shall be carried out by a bailiff. The National Cybersecurity Centre and the Constitution Protection Bureau shall be exempt from the State fee for submitting the decision for enforcement.

(9) If the decisions taken in accordance with Section 34, Paragraph ten, Section 37, Paragraph one, and Section 45, Paragraph one of this Law are not complied with voluntarily, the National Cybersecurity Centre or the Constitution Protection Bureau shall carry out compulsory enforcement thereof in accordance with the Administrative Procedure Law. When carrying out compulsory enforcement of a decision directed towards prohibition of specific activities or activity, the National Cybersecurity Centre or the Constitution Protection Bureau may impose a pecuniary penalty in the amount of not more than EUR 10 000 at a time.

(10) The amount of the pecuniary penalty imposed shall be determined in proportion to the violation committed. When determining the amount of the pecuniary penalty referred to in Paragraph five of this Section, the National Cybersecurity Centre and the Constitution Protection Bureau shall take into account the impact of the failure to comply with the decisions referred to Section 34, Paragraph ten, Section 37, Paragraph one, and Section 45, Paragraph one of this Law on the security of networks and information systems, the duration of the violation, and also other circumstances relevant to the case.

(11) Prior to issuing an enforcement order, the National Cybersecurity Centre and the Constitution Protection Bureau shall notify the addressee in writing that the information necessary for issuing an enforcement 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.

(12) This Section shall not be applied to institutions of direct and indirect administration, other public authorities, and derived public entities.

(13) The paid fine or pecuniary penalty shall be transferred into the State basic budget.

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 17 October 2024, issue the Cabinet regulations referred to in Section 9, Paragraph four, Section 12, Paragraph three, Section 17, Paragraph two, Section 23, Paragraph six, Section 24, Paragraph two, Section 25, Paragraph one, Section 26, Section 28, Paragraph two, Section 29, Section 31, Section 32, Paragraphs two and three, Section 33, Section 34, Paragraphs one, seven, and ten, Section 36, Paragraph one, Section 42, Paragraph three, Section 43, Paragraph two, and Section 44, Paragraph two of this Law.

3. The Cabinet shall, by 1 April 2025, determine the procedures and criteria by which Latvia shall carry out the attribution of cyberattacks.

4. The Cabinet shall, by 1 April 2025, issue the regulations referred to in Section 30, Paragraph two of this Law.

5. Until the day of coming into force of the regulations referred to in Section 17, Paragraph two of this Law but not longer than until 1 January 2025, 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.

6. Until the day of coming into force of the regulations referred to in Section 12, Paragraph three, Section 24, Paragraph two, Section 25, Paragraph one, Section 26, Section 28, Paragraph two, Section 29, Section 30, Paragraph two, Section 34, Paragraphs one, seven, and ten, Section 36, Paragraph one, Section 42, Paragraph three, Section 43, Paragraph two, and Section 44, Paragraph two of this Law but not longer than until 17 October 2024, Cabinet Regulation No. 442 of 28 July 2015, Procedures for the Ensuring Conformity of Information and Communication Technologies Systems to Minimum Security Requirements, and 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 they are not in contradiction with this Law.

7. When performing an initial self-assessment in accordance with Section 22, Paragraph one of this Law, a person shall notify the National Cybersecurity Centre of its conformity with the status of the provider of essential services or the provider of important services not later than until 1 April 2025. If conformity with the status of the provider of essential or the provider of important services has set in after the abovementioned time limit, the person shall notify the National Cybersecurity Centre thereof within the time limit specified in Section 22, Paragraph one of this Law.

8. The list of the providers of essential services and important services referred to in Section 22, Paragraph four of this Law shall be approved by 17 April 2025.

9. The information referred to in Section 23, Paragraph one of this Law on the conformity of a person with the status of the domain name registration service provider shall be notified to the National Cybersecurity Centre not later than until 1 April 2025. If conformity with the status of the domain name registration service provider has set in after the abovementioned time limit, the person shall notify the National Cybersecurity Centre thereof within the time limit specified in Section 23, Paragraph one of this Law.

10. The information referred to in Section 25, Paragraph two of this Law on determination of the cybersecurity manager of the subject shall be initially notified to the National Cybersecurity Centre and the Constitution Protection Bureau not later than until 1 October 2025. If the cybersecurity manager of the subject is determined after the abovementioned time limit, the subject shall notify the National Cybersecurity Centre and the Constitution Protection Bureau thereof within the time limit specified in Section 25, Paragraph two of this Law.

11. Section 34, Paragraphs two, three, four, and five of this Law shall be applicable from 1 July 2025.

12. The self-assessment report referred to in Section 43, Paragraph one of this Law shall be initially submitted to the National Cybersecurity Centre and the Constitution Protection Bureau not later than by 1 October 2025.

13. The providers of essential services which, within the meaning of Article 2(2) of Regulation 2022/2554, are financial entities shall, in respect of the risk management, i.e. management of risks related to third parties, operational resilience, testing, and incident reports, apply the requirements laid down in the legal acts governing the respective field.

Informative Reference to European Union Directives

The Law contains legal norms arising from:

1) 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 (NIS 2 Directive);

2) Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (recast).

The Law shall come into force on 1 September 2024.

The Law has been adopted by the *Saeima* on 20 June 2024.

Acting for the President, Chairperson of the *Saeima* D. Mieriņa

Rīga, 4 July 2024

---

[1] The Parliament of the Republic of Latvia