THE REPUBLIC OF LITHUANIA
CYBERSECURITY LAW NO. XII-1428 AMENDING LAW

11 July 2024 No XIV-2902 Vilnius

Article 1. New version of Law No XII-1428 on Cyber Security of the Republic of Lithuania

wording

Amend Law No XII-1428 on Cyber Security of the Republic of Lithuania and insert the following

Yes:

"LAW ON CYBER SECURITY OF THE REPUBLIC OF LITHUANIA

CHAPTER I GENERAL PROVISIONS

1 **Article 1. Purpose and** application of **the Law**

1. This Law establishes the principles of cybersecurity, the institutions that formulate and implement cybersecurity policy, their functions and powers, the basis for identification of cybersecurity entities and the obligations of cybersecurity entities, the exchange of information and inter-institutional cooperation, the verification and enforcement of cybersecurity entity compliance with the requirements of this Law, the powers of the national cybersecurity certification authority, and the framework for the use of the Secure State Data Transfer Network.

2. This Law, with the exception of Chapter VII, shall not apply to intelligence authorities. This Law shall not apply to credit unions, except credit unions which operate and/or manage networks and information systems independently of the central credit union for the provision of services or activities.

3. The provisions of Articles 14, 15 and 18(1)(1) and/or (2) of this Law do not apply to cybersecurity entities if the applicable European Union legislation requires them to implement cybersecurity risk management measures, reporting major cyber incidents or appointing persons responsible for cybersecurity, and provided that the effect of these requirements is at least equivalent to that of Article 14 of this Law or the implementing acts adopted on the basis thereof, Article 15(1) to (4), Article 18(1)(1) and (4) and/or Article 18(1)(2) and (5)

the impact requirements.

4. The effects of the requirements referred to in paragraph 3 shall be considered equivalent:

1) the impact of the requirements laid down in Article 14 of this Law or in the implementing legal acts adopted on the basis thereof, provided that the cybersecurity risk management measures established include measures aimed at ensuring the security of the network and the information system in terms of availability, authenticity, integrity and confidentiality, and are based on an all-hazards approach, including the security of the network and the information system, in terms of the physical security of the network and the information system, and the security of the environment;

2) the impact requirements set out in Article 15(1) to (4) of this Law, provided that the appointment of a person responsible for cybersecurity is provided for, the impact of which is at least equivalent to the impact requirements set out in Article 15(1) to (4) of this Law;

3) the impact requirements set out in Article 18(1)(1) and (4) of this Law, provided that the cyber incident response service has immediate access, where appropriate, automated and direct, to the incident reports submitted, and that the requirements set out for the reporting of major incidents are at least equivalent in impact to those set out in Article 18(1)(1) and (4) of this Law;

4) the impact requirement set out in Article 18(1)(2) and (5) of this Law, provided that the cyber incident response service is provided with immediate access, where appropriate, automated and direct, to the incident report submitted, and that the requirements for the reporting of incidents by impact are at least equivalent to those set out in Articles 18(1)(2) and (5) of this Law.

5. The Government of the Republic of Lithuania shall, on the proposal of the policy-making ministry in the individual sectors referred to in Annexes 1 and 2 to this Law, approve the list of European Union legal acts which meet at least one of the criteria referred to in paragraph 4 of this Article.

6. The provisions of this Law shall be aligned with the legal acts of the European Union referred to in the following {Annex 3 to this Law.

2 Article. Basic concepts of this Law

1. **"Top-level domain name registration service provider"** means the entity responsible for the administration of a top-level domain, including the registration of a domain name in that domain and its technical operation, including the operation of a name server, the technical maintenance of a database and the distribution of top-level domain name zone files among domain name servers, whether all of those operations are performed by the entity itself or whether part of them are outsourced. An entity shall not be considered to be providing TLD registration services if it uses the TLDs solely for its own purposes.

2. **Cloud service**' means a service of the information society which includes its

administration and wide-area remote access to a variable, scalable base of shared and distributed computing resources, including where such resources are distributed across multiple sites.

3. **Major cyber threat**' means a cyber threat whose technical characteristics suggest that it is likely to have a significant adverse impact on the network and information systems of users of the entity or the service provided by the entity, causing significant material or non-material damage.

4. **'Domain Name Registration Service Provider**' means an entity, or an entity acting on its behalf, that provides domain name registration services, including a provider or reseller of privacy or proxy registration services.

5. Domenq naming system' means a system that hierarchically categorises domain names, identifies Internet services and resources, and enables end-users to use Internet routing and connectivity services to access resources.

6. **'Domain Name System Service** Provider' means an entity that provides publicly available recursive domain name change services to end-users of the Internet, or trusted domain name change services to third parties, other than root domain name server services.

7. **'Data centre service**' means a service provided by a data centre which includes the centralised application, operation and interconnection of information technology and network equipment, the provision of data storage, management and transmission services, and the provision of all energy distribution and environmental control equipment and infrastructure.

8. **'Electronic information hosting services**' means services which consist of the storage of electronic information provided by the recipient of a service at his request.

9. **Internet Exchange Point** - a network device that interconnects more than two separate stand-alone systems to facilitate the exchange of Internet traffic. An Internet data traffic maim point interconnects only autonomous systems and does not require Internet data traffic exchanged between a pair of autonomous systems to be passed through a third autonomous system, nor does it modify or interfere with such traffic.

10. Cyberspace' means the environment consisting of computers and other networking and information technology equipment and the digital data created and/or transmitted on them.

11. **'Cyber incident management**' means the actions and procedures to prevent, detect, analyse and contain a cyber incident or to respond to and recover from a cyber incident.

12. **Cybersecurity risk**' means a potential loss or disruption where

caused by a cyber incident. Cybersecurity risk is expressed as a combination of the magnitude of such loss or disruption and the probability of a cyber incident.

13. **Cybersecurity Entity** means an entity registered in the Cybersecurity Information System.

14. Cyber incident' means an event that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or services provided or accessed through networks and information systems.

15. **National Cyber Security Strategy** - a coherent framework that includes the strategic objectives and priorities set for the Republic of Lithuania in the field of cyber security and the management of their implementation.

16. Distributed Content Delivery Network - a geographically distributed network of servers whose purpose is to ensure, on behalf of content and service providers, the availability, accessibility or rapid delivery of a wide range of digital content and services to Internet users.

17. 'Secure public data network' means a publicly managed electronic communications network that meets specific organisational and technical requirements and is independent of the public electronic communications network.

18. Social networking service platform - an online platform that enables end-users to connect, share content, find each other and the content they publish, particularly through chat, chatbots, video and recommendations, on a variety of devices.

19. **Entity**' means a natural person or a legal person, established and recognised as such under the national law of its place of establishment, who, acting on its own behalf, exercises rights and may be subject to obligations.

20. **Root name server**' means a domain yards server within the top-level domain name system structure that responds to requests by providing a list of the corresponding top-level domain name servers.

21. 'network and information system' means an electronic communications network, any device or interconnected or linked device, one or more of which automatically process digital data in accordance with a programme, or a group or digital data stored, processed, retrieved or transmitted by specified means for the purposes of its management, use, protection and maintenance.

22. 'Network and information system vulnerability' means a deficiency in a network and information system, including deficiencies in information and communication technology products or information and communication technology services, which could lead toa cyber incident or could be exploited to cause a cyber threat.

23. Security of networks and information systems - Capability of networks and information systems

to remain resilient, with a certain level of reliability, to any event that could compromise the availability, authenticity, integrity or confidentiality of the data stored, transmitted or processed, or the availability, authenticity, integrity or confidentiality of the services provided or received, through those networks and information systems.

24. **Managed cybersecurity service provider**' means a managed service provider that carries out, or supports, cybersecurity risk management activities.

25. **Managed service provider**' means an entity that provides services related to the installation, management, operation or maintenance of an information and communication technology product, network, infrastructure, application software or any other network and information system, either in a support capacity or as a proactive administration service at the customer's premises or remotely.

26. **'Near miss cyber incident**' means an event that could have compromised the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed or services provided or accessed through network and information systems, but which was successfully prevented from occurring or did not occur.

27. For the purposes of this Regulation, the terms 'European Cybersecurity Certification Scheme', 'European Cybersecurity Certificate', 'accreditation' and 'conformity assessment body', 'information and communication technology product', 'information and communication technology service', 'information and communication technology process', 'cybersecurity', 'cybersecurity' and 'cybersecurity' shall be understood in the sense in which they appear in Regulation (EU) 2019/881. Definitions "Cybersecurity Community of Excellence", "European Centre of Excellence for Cybersecurity Industry, Technology and Research", "Network of National Coordination Centres" in this Law shall have the meaning given to them in Regulation (EU) 2021/887, "qualified trust service", "qualified trust service provider" in this Law shall have the meaning given to them in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on trust services for electronic communications and electronic transactions in the internal market and repealing Directive 1999/93/EC, as amended. The term "internet search engine" in this Law shall have the meaning given to it in Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on improving the fairness and transparency of the online intermediation service provided to business customers. The terms "standard", "technical specification" in this Regulation shall have the meaning given to them in Regulation (EU) 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC, and

2009/105/EC and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council, as amended. The term 'data' shall be understood as defined in the Law on State Information Resources Management of the Republic of Lithuania.

28. Other terms used in this Law shall have the meaning given to them in the Law on altemative fuels of the Republic of Lithuania, the Law on waste management of the Republic of Lithuania, the Law on renewable energy resources of the Republic of Lithuania, the Civil Code of the Republic of Lithuania, the Law on electronic identification and reliability of electronic operations of the Republic of Lithuania, the Law on electronic communications of the Republic of Lithuania, the Law on electricity of the Republic of Lithuania, the Law on pharmaceutical products and the Law on electronic communications of the Republic of Lithuania.

Law of the Republic of Lithuania, the Law of the Republic of Lithuania on the Collection of Financial Instruments, the Law of the Republic of Lithuania on Natural Gas, the Law of the Republic of Lithuania on Railway Transport Code, the Law of the Republic of Lithuania on Drinking Water, the Law of the Republic of Lithuania on Drinking Water Supply and Wastewater Management, the Law of the Republic of Lithuania on the Information Society Service, the Law of the Republic of Lithuania on Crisis Management and Civil Safety, the Law of the Republic of Lithuania on Science and Studies, the Law of the Republic of Lithuania on the Protection of Objects of Importance for National Security, the Law on Petroleum Products and Petroleum State Reserves of the Republic of Lithuania, the Law on Prohibition of Unfair Commercial Practices for Consumers of the Republic of Lithuania, the Law on Postal Services of the Republic of Lithuania, the Law on Safe Navigation of the Republic of Lithuania, the Law on Small and Medium Enterprises of the Republic of Lithuania, the Law on the Basis of Transport Activities of the Republic of Lithuania, the Law on Management of Information Resources of the Republic of Lithuania, the Law on Public Administration of the Republic of Lithuania, the Law on Intelligence of the Republic of Lithuania.

3 Article. Principles of cybersecurity

1. Cybersecurity shall be based on the following cybersecurity principles:

1) non-discrimination in cyberspace - the provisions of the law are applied and the protection of the rights protected by the law is ensured equally in both physical and cyberspace;

2) cybersecurity risk management - cybersecurity risk management measures must ensure that the risks regularly assessed by the cybersecurity entity are managed;

3) proportionality of cybersecurity - the cybersecurity risk management measures applied must not restrict the activities of the cybersecurity actor beyond what is necessary to ensure cybersecurity;

4) the primacy of the public interest - cybersecurity risk management measures must first and foremost ensure the protection of the public interest, but must not inherently infringe individual rights

the rights and legitimate interests of users, cybersecurity actors or disproportionately restrict their freedom;

5) standardisation and technological neutrality - when implementing cybersecurity risk management measures, cybersecurity actors are encouraged to follow national, European Union and other international standards and technical specifications for network and information system security, without requiring or favouring any particular type of technology;

6) Subsidiary - cybersecurity of networks and information systems and the services they provide is the responsibility of the cybersecurity entities that operate and provide the services they provide. In areas that fall within the exclusive competence of the cybersecurity entity, the authorities shall only act in the formulation and implementation of cybersecurity policy when the cybersecurity of the network and information system and the services provided through it is not ensured by the cybersecurity entities that operate and provide services through these systems.

2. All the principles referred to in paragraph 1 of this Article shall be taken into account in the application of the legal provisions governing cybersecurity. These principles shall be mutually reinforcing and shall not give priority to any one of them.

II CHAPTER 1

CYBERSECURITY POLICY DEVELOPMENT AND IMPLEMENTATION

4 Article 3. Institutions for the development and implementation of cybersecurity policy

1. The cybersecurity policy shall be formulated taking into account the priorities and objectives of the long-term national security policy set out in the National Security Strategy approved by the Seimas of the Republic of Lithuania, the strategic goals and objectives set out in the National Plan of Progress approved by the Government, and the priorities and directions of implementation set out in the National Programme for Strengthening and Development of the National Defence System approved by the Seimas and the National Programme for Development of Cybersecurity approved by the Government. The strategic planning documents referred to in this paragraph, or parts thereof, together with this Law and its implementing legislation, shall constitute the National Cyber Security Strategy.

2. The Ministry of National Defence of the Republic of Lithuania shall formulate the cybersecurity policy, organise, control and coordinate its implementation. The Ministry of Foreign Affairs of the Republic of Lithuania shall be involved in the formulation of the cyber security policy to the extent necessary to determine the legal regulation of the application of diplomatic measures in response to cyber threats and cyber incidents. The National Cyber Security Centre shall be involved in the formulation of cyber security policy to the extent necessary to determine the following for the performance of its functions under this Law

the legal regulation of the operation and maintenance of cybersecurity entities.

3. The National Cyber Security Centre, the Lithuanian Police and the State Data Protection Inspectorate implement cyber security policy.

5 Article. Powers of the Ministry of National Defence in the field of cyber security

The Ministry of National Defence shall, in addition to the formulation of the cyber security policy as provided for in Article 4(2) of this Law and the performance of other functions set out in this Law, cooperate with the relevant institutions of the North Atlantic Treaty Organisation (hereinafter referred to as "NATO") and of the European Union, as well as with the institutions of the NATO member states and of the European Union member states, and with the international institutions in the field of cyber security.

6 Article 1. Cybersecurity Council

1. The Cybersecurity Council (hereinafter referred to as the Council) is a permanent collegial independent advisory body acting on a public basis, which draws on the knowledge and best practices of the members of the Council and provides suggestions to the Ministry of National Defence for its work.1:

1) cybersecurity policy priorities, direction of development, expected results and means of implementation;

2) opportunities for cooperation between the public sector, businesses and research and academic institutions in the field of cybersecurity;

3) cybersecurity risk management tools, cyber incident management and cybersecurity enhancement.

2. The members of the Council shall be representatives of the institutions which formulate, participate in the formulation and implementation of the cybersecurity policy, representatives of the authority responsible for the identification of the cybersecurity entity, as referred to in Annexes 1 and 2 to this Law, representatives of associations representing cybersecurity entities, representatives of scientific and study institutions and members of the Cybersecurity Community, as referred to in Article 23 of this Law.

3. The Council shall be chaired by a representative of the Ministry of National Defence.

4. The Council shall be constituted, its institutional and personal composition and its rules of procedure approved by the Minister of National Defence.

5. The Council shall be physically and technically serviced by the Ministry of National Defence or an institution authorised by the Minister of National Defence.

6. The Council shall have the following rights in order to achieve the objectives of its activities:

1) to obtain from State and municipal institutions and bodies the information necessary to deal with the matters falling within its competence;

2) to organise meetings, conferences and other events.

7 Art. National Cyber Security Centre

1. The National Cyber Security Centre is an agency under the Ministry of National Defence.

2. The National Cyber Security Centre shall implement the cyber security policy:

1) apply cyber threat detection tools in cyberspace to assess the resilience of networks and information systems to cyber incidents;

2) monitors, collects and analyses information on cyber threats, network and information system vulnerabilities (hereafter referred to as "vulnerabilities"), cyber incidents and near misses;

3) manage cyber incidents in accordance with the National Cyber Incident Management Plan approved by the Government;

4) provide early warnings, alerts, notifications and information exchange to cybersecurity actors and stakeholders on cyber threats, vulnerabilities, cyber incidents and near misses;

5) provide assistance to cybersecurity actors in the monitoring of the jq network and information system;

6) in order to stop the impact of a cyber incident on the security of the cybersecurity entity's network and information system, instruct the public electronic communications network and/or the providers of public electronic communications services, electronic marketplace, internet search engine, cloud services, restrict the provision of a public electronic communications network and/or a public electronic communications service, an electronic marketplace, an internet search engine, a cloud service, an electronic information hosting service, for a period of not more than 48 hours to providers of electronic information hosting services. The National Cyber Security Centre shall notify the Communications Regulatory Authority of the Republic of Lithuania no later than the next working day of the instructions given to providers of a public electronic communications network and/or a public electronic communications service pursuant to this point;

7) in order to eliminate cyber threats or to stop their spread, instruct public electronic communications networks and/or providers of public electronic communications services and/or providers of domain name registration services to block a website, distributing malware, fraudulently collecting network and information system login data and/or used for the coordination and execution of cyber incidents, domain names, as well as other domain names created for the purpose of carrying out the aforementioned website activities. The owner of the website shall have the right to appeal to the court against the order of the National Cyber Security Centre to block the domain name of the website, as provided for in the Civil Procedure Code of the Republic of Lithuania

procedure;

8) apply bi-annual cybersecurity measures in the event of a cyber incident;

9) inspect the network and information systems operated and/or managed by the cybersecurity entityq systems to identify vulnerabilities;

10) coordinate the disclosure of vulnerabilities;

11) collecting and analysing cyber incident investigation data, conducting cybersecurity risk and cyber incident analysis, as well as ensuring that the cybersecurity policy maker, the implementing authority and the cybersecurity entity are kept informed of the situation in the field of cybersecurity;

12) when it is necessary to inform the public in order to prevent a cyber incident or to manage an ongoing cyber incident or cyber threat, after consulting the cybersecurity actor that reported the cyber incident, inform the public about the cyber incident and/or cyber threat, if possible, indicating the action to be taken in response to the cyber incident and/or cyber threat, or require the reporting cybersecurity entity to do so;

13) participate in crisis management of cyber incidents in accordance with the procedures laid down in the Law on Crisis Management and Civil Protection;

14) in coordination with the National Crisis Management Centre, notify the European Competent Authorities of crises related to cyber incidents which the Republic of Lithuania alone is unable to manage;

15) participate in the activities of the European Union and NATO Cyber Incident Response Networkq and provide mutual assistance, within their respective capabilities and competences, to other members of this network upon request;

16) monitor the compliance of the cybersecurity entity with the cybersecurity risk management measures;

17) advise the cybersecurity entity on the selection and application of cybersecurity risk management measures;

18) cooperate with, and have the right to use, international organisations and institutions of the European Union member states, NATO member states and other state institutions and organisations that tg endorse cybersecurity policy, and have the right to use them in the performance of the cybersecurity functions provided for in this Law and in other legal acts;

19) develop national projects to strengthen cyber security in cooperation with businesses, research and study institutions, national, European Union Member States, NATO Member States and other governmental institutions and organisations, international organisations, non-governmental organisations and cyber security entities;

20) perform other functions set out in this Law.

3. The National Cyber Security Centre shall have the right to use an independent auditor, audit firm or other body that meets the requirements of independence, impartiality and good repute set by the National Cyber Security Centre, as laid down in the methodology referred to in Article 14(8) of this Law, for the purpose of carrying out the functions referred to in paragraph 2(16) of this Article, to carry out a cyber security audit. The cybersecurity audit shall verify the cybersecurity of the network and information system operated and/or managed by the cybersecurity entity.

4. Cybersecurity entities and other entities shall have the right to appeal against the measures applied and instructions given by the National Cyber Security Centre to the court in accordance with the procedure established by the Law on Administrative Procedure of the Republic of Lithuania, except for the cases specified in this Law, where another appeal procedure shall apply.

5. The National Cyber Security Centre shall meet the following requirements:

1) The communication channels of the National Cyber Security Centre shall be easily accessible, avoiding critical points of malfunctioning;

2) a number of ways of contacting the National Cyber Security Centre at any time shall be established, and the cyber security actors and other authorities referred to in Article 20 of this Law shall be informed of these ways and channels of communication;

3) the premises of the National Cyber Security Centre and the supporting information systems shall be located in places that do not jeopardise the continuity of the functions performed by the National Cyber Security Centre;

4) The National Cyber Security Centre shall have a request management and transmission system that ensures efficient and effective transmission of requests;

5) The National Cyber Security Centre must ensure the confidentiality and reliability of its activities;

6) The National Cyber Security Centre must be sufficiently staffed to ensure its availability at all times;

7) The staff of the National Cyber Security Centre must be adequately trained to perform its functions;

8) The National Cyber Security Centre must have secondary systems and a back-up workspace to ensure the continuity of the functions of the National Cyber Security Centre.

6. The Ministry of National Defence shall ensure that the National Cyber Security Centre has sufficient capacity and resources to carry out the functions set out in paragraph 2 of this Article, to meet the requirements set out in paragraph 5 of this Article, and to develop the technical capabilities of the National Cyber Security Centre.

8 Article 2. Crisis and emergency preparedness in the field of cybersecurity

1. The National Cyber Security Centre shall maintain data on cybersecurity entities, other bodies and economic operators entrusted with critical tasks in the management of cyber incidents in the event of an emergency in cyberspace.

2. The National Cyber Security Centre shall approve a cyber security exercise plan for the organisation of cyber security exercises and training for the cyber security entities referred to in paragraph 1 of this Article, other ţinstitutions and economic operators, in order to ensure preparedness for crises, emergencies and cyber security situations.

9 Article 2. Powers of the State Data Protection Inspectorate in the field of cybersecurity

The State Data Protection Inspectorate implements the cybersecurity policy in the field of personal data protection and performs the tasks of a supervisory authority as laid down in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the 'General Data Protection Regulation', as amended).

10 Article 2. Police powers in the field of cybersecurity

1. The police shall, in the implementation of the cybersecurity policy:

1) receive and process data and/or information on cyber incidents for the purposes of prevention, analysis, investigation or detection of criminal activities;

2) have the right to obtain from the cybersecurity entity the information needed to analyse and assess whether a cyber incident has the potential to constitute a criminal offence. Cybersecurity entities shall be obliged to provide the information referred to in this point to the police upon request;

3) have the right, where the recipient of a public electronic communications network and/or a public electronic communications service, an electronic information hosting service, an electronic marketplace, an Internet search engine, a cloud service is potentially involved in or the network and information technology equipment used by the recipient is potentially used for a criminal offence, to instruct, without court sanction, the provider of the public electronic communications network and/or the provider of the public electronic communications service, an electronic information hosting service provider, an electronic marketplace, an Internet search engine, a cloud service provider, for a period of not more than 48 hours, and for a longer period of time, with the sanction of the district court, to restrict the public electronic communications network and/or public electronic communications service, an electronic information hosting service, an electronic marketplace, an Internet

the provision of a search engine, a cloud service to the recipient of thisq service, and/or order measures to address the causes of criminal activity in cyberspace. In these cases, a reasoned order shall be submitted to the judge for confirmation of the lawfulness or reasonableness of the action. If the period of limitation of the provision of services referred to in this point expires on a day of rest or public holiday, the application shall be submitted no later than the working day following the day of rest or public holiday. The judge shall examine the application and issue a decision on the legality or reasonableness of the action referred to in the application at the latest within 3 working days from the date of submission of the application. If the judge does not confirm the legality or reasonableness of the action referred to in the application by a reasoned order, the order shall be suspended immediately;

4) shall have the right to instruct a provider of a public electronic communications network and/or a public electronic communications service, a provider of an electronic information hosting service, an electronic marketplace, an internet search engine, a cloud service, to retain, in relation to the services they provide, information which makes it possible to determine the type of communications service used, the means used and the time of use, the identity of the recipient of the service, the postal address, the geographical location, the communication number, information on bills and payments made on the basis of the service contract or agreement, and other information at the place of installation of the communication service available under the service contract or agreement, to obtain that information and, where there is a reasoned order from a court of law, to receive the recipient's traffic data and to control the content of the information communicated in accordance with the present paragraph.

2. Police orders to restrict the provision of services to a recipient, and/or orders to take measures to eliminate the causes of criminal activity in cyberspace, and/or orders to service providers to preserve information relating to the services they provide, must be executed within a maximum of 8 hours from the time of the police order, and in cases of extreme urgency as soon as possible, and in any case within a maximum of one hour from the time of receipt of the order.

III CHAPTER

IDENTIFICATION OF THE CYBERSECURITY ACTOR AND RESPONSIBILITIES OF THIS ACTOR

11 Article 1. Cybersecurity actors

1. The status of a cybersecurity entity shall be granted to entities registered in the Cybersecurity Information System that meet at least one of the identification criteria for a general or specific cybersecurity entity as set out in paragraphs 3 to 5 of this Article, and that operate and/or manage networks and information systems for the provision of the services or activities referred to in these paragraphs. Taking into account the potential negative impact that a cyber incident may have on

the network and information systems managed and/or operated by a cybersecurity entity, cybersecurity entities shall be divided into essential cybersecurity entities (hereinafter referred to as 'essential entities') and critical cybersecurity entities (hereinafter referred to as 'critical entities').

2. Cybersecurity entities shall only be subject to the obligations imposed on cybersecurity entities upon registration in the Cybersecurity Information System.

3. General criteria for the identification of material entities:

1) the entity provides services and/or carries out activities in the sectors listed in Annex 1 to this Law and exceeds the thresholds for the number of average employees and financial data laid down in the Law on the Development of Small and Medium-sized Enterprises;

2) the entity provides qualified trust assurance services, top-level domain name registration services or domain name system (DNS) services in the digital infrastructure sector referred to in Annex 1 to this Law, with the exception of root name serveriq operators;

3) the entity provides a public electronic communications network or public electronic communications services in the digital infrastructure sector referred to in Annex 1 to this }Law and is considered a medium-sized enterprise within the meaning of the Law on the Development of Small and Medium-sized Enterprises;

4) the entity is recognised as an entity of critical importance in accordance with the procedure laid down by the Law on Crisis Management and Civil Protection;

5) the entity provides services and/or carries out activities in the sector of public administration referred to in Annex 1 of this Law and is considered a central public administration entity or a regional administration entity or a municipal administration entity within the meaning of the Law on Public Administration;

6) the entity manages and/or maintains critical and/or important State information resources in accordance with the procedure laid down in the Law on State Information Resources Management;

7) the entity is considered to be an undertaking of national security importance or the network and information system operated and/or managed by the entity is included in the list of installations and assets of national security importance.

4. General criteria for the identification of a critical entity:

1) the entity provides services and/or carries out activities in the sectors listed in Annex 2 to this Law, exceeds the thresholds defining the number of employees and the financial data set out in the Law on Small and Medium-sized Enterprises Development, and the annual income of the services and/or activities provided by the entity as referred to in this point exceeds 50 per cent of the entity's annual income;

2) the entity provides services and/or carries out activities in the sectors listed in Annex 1 to this Law and exceeds the thresholds defining the number of employees and the financial data,

but does not exceed the thresholds for the average number of employees and financial data as laid down in the Law on the Development of Small and Medium-sized Enterprises;

3) the entity provides unqualified trust assurance services in the digital infrastructure sector referred to in Annex 1 to this Law and is considered a medium, small or micro enterprise within the meaning of the Small and Medium-sized Enterprise Act;

4) the entity provides public electronic communications networks or public electronic communications services in the digital infrastructure sector referred to in Annex 1 to this Law and is considered a small or very small enterprise within the meaning of the Lawon the Development of Small and Medium-sized Enterprises;

5) the entity owns and/or manages public information resources;

6) the entity provides domain name registration services;

7) the entity provides electronic information hosting services.

5. Specific criteria for the identification of a cybersecurity entity:

1) the entity is the sole provider of a service which is necessary to ensure the performance of a public or economic activity of particular importance in the Republic of Lithuania;

2) the disruption of the service provided by the entity could have a significant impact on public security, public safety or public health;

3) the disruption of a service provided by the entity could pose a significant systemic risk in sectors where such disruption could have a cross-border impact;

4) the entity is of critical importance in terms of its relevance to a specific sector or service or to other interdependent sectors at national or regional level;

5) an entity in the sector of public administration referred to in Annex 1 of this Law provides services and/or carries out activities which, if disrupted, could have a significant impact on the state, institutions or the population, and is considered a territorial public administration entity or a regional administration entity or a self-government administration entity in accordance with the Law on Public Administration;

6) the disruption of a service provided by the entity could have a significant impact on the essential service and/or activities provided by the entity;

7) the entity is a provider of a service which is necessary for the performance of vital State functions and State mobilisation tasks;

8) the entity carries out critical research and experimental development activities in the sector of scientific research referred to in Annex 2 to this Law.

6. The Government shall establish a methodology for identification according to specific criteria, which shall classify an entity as essential or important. Only essential entities shall be identified according to the criterion referred to in paragraph 5(5) of this Article, and according to paragraph 5 of this Article

The criterion referred to in point 8 of paragraph 5 shall identify only essential entities.

7. If an entity meets at least one of the criteria specified in paragraphs 3 or 5 of this Article for the identification of a material entity, the entity shall be deemed to be a material entity irrespective of its compliance with the criteria for a significant entity.

12 Article 2. Jurisdiction and territoriality

1. For the purposes of identifying a cybersecurity entity, the jurisdiction of the Republic of Lithuania shall be deemed to include:

1) entities registered in the Republic of Lithuania, except:

a) public administration bodies that are subject to the jurisdiction of another country;

b) the entities referred to in point 3 of this paragraph whose head office is located outside the Republic of Lithuania;

2) public administration entities which the Republic of Lithuania has established in other States;

3) providers of DNS services, providers of top-level domain name registration services, providers of domain name registration services, providers of cloud services, providers of data centre services, providers of distributed content delivery network services, providers of managed services, providers of managed cybersecurity services, providers of electronic marketplaces, Internet search engines or social networking platform services, which have their principal place of business in the Republic of Lithuania;

4) providers of a public electronic communications network and/or a public electronic communications service providing these services in the Republic of Lithuania.

2. The head office referred to in paragraph 1(3) of this Article shall be deemed to be located in the Republic of Lithuania if the entities referred to in paragraph 1(3) of this Article are rebistructed or established in the Republic of Lithuania. The head office referred to in paragraph 1(3) of this Article shall be deemed to be

shall be established in the Republic of Lithuania if decisions relating to cybersecurity risk management measures are taken in the Republic of Lithuania. If the Member State of the European Union in which such decisions are taken is not identified, or if such decisions are not taken in the European Union, the head office shall be deemed to be in the Republic of Lithuania when the Republic of Lithuania

Cybersecurity risk management measures are implemented. If the Member State of the European Union in which the cybersecurity risk management measures are implemented is not identified, the head office shall be deemed to be in the Republic of Lithuania if the entity has an establishment in the Republic of Lithuania, where the majority of the entity's employees are employed within the European Union.

3. Where the entity referred to in paragraph 1(3) is not established in the European Union but provides services in the Republic of Lithuania, it must designate a European Union

a natural or legal person established to act only as a DNS service provider, a top-level domain name registration service provider, a domain name registration service provider, a cloud service provider, a data centre service provider, a distributed content delivery network service provider, a managed service provider, and a managed cybersecurity service provider, an electronic marketplace service provider, an internet search engine service provider or a social networking platform service provider that is not established in the European Union, on behalf of which the National Cyber Security Centre may apply to act in place of the entity for the purpose of performing that entity's duties under the Act ("the agent") in the European Union. The representative referred to in this paragraph must be established in one of the Member States of the European Union in which the services are provided. If the entity referred to in paragraph 1(3) of this Article appoints a representative in the Republic of Lithuania, or does not appoint a representative but provides services in the Republic of Lithuania, such entity shall be deemed to be under the jurisdiction of the Republic of Lithuania.

13 Article 2. Register of cybersecurity entities

1. The subject of the register of cybersecurity entities shall be cybersecurity entities.

2. The Register of Cybersecurity Entities shall be maintained in the Cybersecurity Information System.

3. The Cybersecurity Entity Register shall contain the following basic data on cybersecurity entities:

1) if the cybersecurity entity is a legal person, the name, legal entity code, legal form, economic field(s) of activity, and the address of the head office, and if the cybersecurity entity is not established in the European Union, the name, legal form, economic field(s) of activity, and the name and address of the representative appointed in accordance with Article 12(3) of this Law. If the cybersecurity entity is a DNS service provider, a top-level domain name registration service provider, a cloud service provider, a data centre service provider, a distributed content delivery network service provider, a managed security service provider, a managed cybersecurity service provider, an electronic marketplace service provider, an Internet search engine and social networking platform service provider (hereinafter referred to as a 'special entity'), or is a domain name registration service provider, and the addresses of other legal entities in the European Union;

2) if the cybersecurity entity is a natural person - the name, surname, personal identification number and business address of the cybersecurity entity;

3) the contact details (e-mail address) of the cybersecurity entity (including, if it is not established in the European Union, of the representative appointed in accordance with Article 12(3) of this Law)

address, communication number);

4) the services provided and/or activities carried out by the cybersecurity entity which meet the criteria referred to in Article 11(3) to (5) of this Law;

5) Internet Protocol (IP) addresses used by the cybersecurity entity;

6) the countries in which the cybersecurity entity provides services and/or carries out activities listed in the sectors and subsectors referred to in Annexes 1 and 2 to this Law;

7) network and information systems relevant to the provision of the service or activities of the cybersecurity entity;

8) the sector referred to in Annexes 1 and 2 to this Law in which the cybersecurity entity operates or provides services, and its subsector.

4. An entity that meets the criteria for identification of a cybersecurity entity set out in Article 11(3) to (5) of this Law shall provide the data specified in the regulations of the Cybersecurity Information System approved by the Minister of National Defence to the Cybersecurity Information System Data Processor. The data shall be provided in accordance with the procedure laid down in these Regulations.

5. Cybersecurity entities shall be registered and de-registered by the Cybersecurity Information System Data Manager in accordance with the procedure laid down in the Cybersecurity Information System Regulations. Cybersecurity entities shall be assigned to the sectors, sub-sectors and entity classes referred to in Annexes 1 and 2 to this Law in accordance with the classification of economic activities according to the procedure laid down in the Cybersecurity Information System Regulations.

6. The authorities referred to in Annexes 1 and 2 to this Law, responsible for the identification of a cybersecurity entity, shall validate the data of the Cybersecurity Information System Data Processor referred to in paragraph 3 of this Article on cybersecurity entities, as well as the cybersecurity entities identified in accordance with the methodology of identification according to the specific criteria established by the Government, in accordance with the procedures laid down in the Cybersecurity Information System Regulations.

7. Entities, as well as other public authorities, public bodies, state-owned enterprises, public bodies, municipally owned enterprises and municipalities, shall be identified and registered in the cases and according to the procedures set out in the Cybersecurity Information System Regulations

} institutions shall provide the data referred to in paragraph 3 of this Article and other information summarising these data necessary for the registration of cybersecurity entities to the Cybersecurity Information System Data Processor free of charge.

8. If a cybersecurity entity does not meet the criteria referred to in Article 11(3) to (5) of this Law, it shall be deregistered from the Cybersecurity Information System. A cybersecurity entity shall be deregistered from the Cybersecurity Information System

within 20 working days from the date on which the Cybersecurity Information System Data Processor receives information that the cybersecurity entity no longer meets the criteria referred to in Article 11(3) to (5) of this Law.

9. Entities shall have the right to appeal against the decision to register or not to register them in the Cybersecurity Information System, as well as against the decision to de-register them in accordance with the procedure laid down in the Law on Administrative Procedure.

10. A cybersecurity entity shall cease to be subject to the obligation for cybersecurity entities referred to in this Law as from its de-registration from the Cybersecurity Information System.

14 Article 2. Cybersecurity risk management measures

1. Cybersecurity entities shall ensure that the network and information system used for the performance of the activities or provision of the services that meet the criteria referred to in Article 11(3) to (5) of this Law complies with the cybersecurity risk management measures:

1) cybersecurity requirements to be approved by the Government, except in the cases referred to in paragraph 4 of this Article;

2) Implementing acts adopted by the European Commission.

2. Cybersecurity entities shall be obliged to implement the cybersecurity requirements referred to in paragraph 1(1)(1) of this Article within a period of time set by the Government of at least 12 months from the date of their registration in the Cybersecurity Information System. In setting the time limit, the Government must take into account the cybersecurity requirements the human and financial resources of the cybersecurity entity required for implementation.

3. Cybersecurity entities are required to submit to the National Cybersecurity Centre, in accordance with the procedures laid down in the Cybersecurity Information System Regulations, the data on the implementation of the cybersecurity risk management measures referred to in those Regulations.

4. A special entity shall be obliged to ensure that the networks and information system it uses comply only with the cybersecurity risk management measures referred to in point 2 of paragraph 1 of this Article.

5. The cybersecurity requirements shall include the following elements:

1) cybersecurity risk analysis, network and information system cybersecurity policies;

2) the person responsible for cybersecurity as referred to in Article 15 of this Law and the head of the cybersecurity entity or his/her delegate;

3) cyber incident management;

4) business continuity;

5) supply chain security, including aspects relating to the relationship between each cybersecurity entity and its direct suppliers or service providers;

6) network and information system acquisition, development and maintenance security, including vulnerability management and disclosure;

7) policies and procedures for the effectiveness of cybersecurity requirements
to assess the effectiveness of the cyber security policy;

8) cyber hygiene practices and regular cybersecurity training;

9) policies and procedures for the use of cryptography and encryption;

10) human resources security, network and information system access control policies and asset management;

11) the use of a ke1iq active authentication or persistent authentication solution, secure voice, video and text communications and a secure emergency communications system within the entity;

12) a policy for the provision and management of legal and access to the network and information system operated and/or managed by the cybersecurity entity to users, administrators, suppliers, sub-suppliers and other entities of the network and information system operated and/or managed by the cybersecurity entity, and/or digital data;

13) other cybersecurity requirements applicable to individual sectors or groups of individual cybersecurity entities, based on the identified cybersecurity risks of the individual sector.

6. The head of the cybersecurity entity or his/her delegate shall ensure that the cybersecurity entity complies with the obligations imposed on it by this Law and shall supervise compliance with those obligations. The head of the cybersecurity entity shall, when authorising the person referred to in this paragraph, ensure that he/she has the necessary means to exercise the specified power.

7. The members of the governing body of the cybersecurity entity, the head and his/her delegate, if any, or the cybersecurity entity, if it is a natural person, shall be obliged to undergo cybersecurity training at least once every 2 years in accordance with the procedure established by the head of the National Cyber Security Centre and to ensure that the employee, if any, of the cybersecurity entity receives continuous cybersecurity education.

8. Cybersecurity entities shall conduct a cybersecurity audit at least once every 3 years in accordance with the methodology for conducting cybersecurity audits approved by the National Cybersecurity Centre. Cyber security audits shall be carried out by independent information system security compliance auditors certified by a generally recognised international organisation, auditing companies or other bodies, who have undergone training and passed a qualification examination in accordance with the procedure laid down by the Head of the National Cyber Security Centre

persons who meet the requirements of independence, impartiality and good repute laid down in the Methodology for conducting cyber security audits of the National Cyber Security Centre (hereinafter referred to collectively as 'auditors'). Auditors may not be entrusted with the assessment of the security of the network and information system operated and/or managed by the entity in which the auditor works.

15 Article. Persons responsible for cybersecurity

1. The head of the cybersecurity entity or his/her delegate must appoint a cybersecurity manager directly reporting to the head of the cybersecurity entity, responsible for ensuring the compliance of the cybersecurity entity with the requirements set out in Articles 14 and 18 of this Law and for performing other functions set out in the legal acts regulating cybersecurity.

2. The head of the cybersecurity entity or his/her delegate must designate a security officer responsible for ensuring compliance with the requirements laid down in Articles 14 and 18 of this Law and for carrying out the other functions laid down in the legal acts on cybersecurity for the specific network and information system.

3. The Head of Cybersecurity may act as the Safety }Authority. The Cybersecurity Manager may be designated to be responsible for the implementation of the requirements set out in Articles 14 and 18 of this Law for multiple cybersecurity entities. The Security Officer may be designated to be responsible for ensuring that the network and information system comply with the requirements laid down in Articles 14 and 18 of this Law. The operator of the network and information system shall have the right to delegate the appointment of a security officer to the operator of that network and information system.}

4. A cybersecurity entity shall be allowed to procure services from a supplier that perform the functions of a cybersecurity manager and/or a security delegate. {The acquisition of the services referred to in this paragraph shall ensure compliance with the requirements laid down in Articles 14 and 18 of this tLaw.

5. Cybersecurity Manager and Safety Officer:

1) Must meet the requirements of good repute for public servants set out in the Law on the Civil Service of the Republic of Lithuania;

2) must not have an administrative penalty for infringements of the law in the areas of network and information system and personal data processing and privacy protection, less than one year after the imposition of the penalty;

3) have at least 2 years' experience in the field of information technology, cybersecurity or network and information systems, or a higher education diploma, an internationally recognised certificate of competence or, in accordance with the procedure laid down by the Head of the National Cyber Security Centre, have undergone training and have passed a cyber security test

the examination of the Head of Cyber Security.

6. Where the cybersecurity entity is a natural person, it shall not be subject to the requirements set out in this Article.

16 Article 3. Technical measures for cybersecurity

1. The National Cyber Security Centre shall deploy and manage technical cyber security measures in the networks and information systems of the material entity as part of the monitoring of the network and information system operated and/or managed by the material entity in order to identify cyber threats and cyber incidents. Technical cybersecurity measures may be deployed at the request of the entity to manage cyber incidents on network and information systems owned and/or operated by the entity. The measures referred to in this paragraph shall be deployed and used in such a way as to ensure the security, uninterrupted operation, secrecy, confidentiality, availability and resilience of the data and information of the cybersecurity entity and the network and information system operated and/or maintained by the cybersecurity entity, the adequate protection of the rights and legitimate interests of the cybersecurity entity and of other entities.

2. The Minister of National Defence shall establish a procedure for the implementation and management of technical cyber security measures in networks and information systems managed and/or operated by the cyber security entity, approve a plan for the implementation of technical cyber security measures, which shall specify the technical cyber security measures and the data (if any) to be processed by these measures.

3. The technical cybersecurity measures implemented by the National Cybersecurity Centre shall be maintained, operated and repaired at the expense of the National Cybersecurity Centre.

4. Covered entities shall enable the National Cyber Security Centre to deploy and manage technical cyber security measures.

17 Article 2. Requirements for the registration of top-level domain names and the provision of a domain name registration service

Cybersecurity entities that are Top Level Domain Name Registration Service Providers and Domain Name Registration Service Providers must:

1) to contribute to the security, stability and resilience of the DNS, to compile information that allows bütq to identify and contact the holders of domain names and the contact persons who administer top-level domain names bearing domain names in bütq, in accordance with

Regulation (EU) 2016/679 when processing personal data. Such information includes:

a) the domain name;

b) the date of registration of the domain;

c) the name of the legal entity or the name of the natural person holding the domain name; contact details (email address, contact number);

d) the e-mail address and contact number of the contact person administering the domain name, if different from those of the domain name holder;

2) apply policies and procedures, including verification procedures, to ensure that the domain name registration database contains accurate and complete information;

3) make the policies and procedures referred to in paragraphs 2 and 5 of this Article publicly available on a regular basis on its website or, where it does not have one, through other means of public information;

4) make publicly available on its website or, if it does not have one, on other means of public communication, the registration details of the domain name, which are not personal data, no later than 72 hours after the registration of the domain name;

5) upon receipt of legitimate and justified requests for lawful access to domain name registration data that constitutes personal data from the requesting entity, in accordance with the applicable disclosure policies and procedures, to provide access to the specific domain name registration data in accordance with the procedures set out in Regulation (EU) 2016/679. Responses shall be provided to the requesting entity at the latest within 72 hours of receipt of the access request;

6) cooperate with each other in order not to duplicate the collection of domain name registration data.

18 Article 2. Notification of cyber incidents

1. Cybersecurity actors are obliged to report to the National Cybersecurity Centre:

1) a major cyber incident affecting the activities and/or services provided that meet the criteria referred to in Article 11(3) to (5) of this Law;

2) cyber incidents that do not meet the criteria of a major cyber incident as referred to in paragraph 2 of this Article and that have an impact on activities and/or services provided that meet the criteria referred to in Article 11(3) to (5) of this Law, within the timeframe set out in the national cyber incident management plan, and to provide the information set out in that plan.

2. A cyber incident shall be considered as major in at least one of the following cases:

1) where, as a result of a cyber incident, a cybersecurity entity has suffered or is likely to suffer a significant service disruption or financial loss;

2) where the cyber incident has affected or is likely to affect other natural or legal persons, causing significant material or non-material damage.

3. The cases in which a cyber incident is considered to be serious are further specified in implementing legislation adopted by the European Commission.

4. The notification of a major cyber incident shall include:

1) an early warning, as soon as possible, but at the latest within 24 hours of becoming aware of a major cyber incident, indicating, to the extent possible, whether the major cyber incident is suspected to have been caused by unlawful or malicious acts, and whether it has the potential to have a transnational impact;

2) without delay, but at the latest within 72 hours of becoming aware of the major cyber incident, a cyber incident report, updating, to the extent possible, the information referred to in point (1) of this paragraph and indicating the initial assessment of the major cyber incident, including its severity and impact, as well as evidence of a breach, if any;

3) at the request of the National Cyber Security Centre, an interim report of the corresponding updated situation data within the submission deadline specified by the National Cyber Security Centre;

4) no later than one month from the date of notification of the cyber incident referred to in point 1 of this paragraph, a final report containing this information:

a) a detailed description of the cyber incident, including its severity and impact;

b) the threat or root cause that allowed the cyber incident to occur,

a description of the nature of the cyber incident;

c) the measures taken and implemented to mitigate the impact of the cyber incident;

d) the cross-border impact of the cyber incident, if any;

5) if, at the time of submission of the final report referred to in point 4 of this paragraph, the cyber incident is still ongoing, a progress report shall be submitted and the final report shall be submitted within one month of the date on which the cyber incident was contained.

5. The national cyber incident management plan shall establish:

1) the timeframes within which cyber incidents other than those referred to in paragraph 1(1) of this Article shall be reported;

2) the information to be communicated when reporting cyber incidents other than those referred to in point (l)(1) of this Article;

3) the ways and means of reporting cyber incidents;

4) the action to be taken by the institution following the receipt of information on cyber incidents;

5) more detailed cases where a cyber incident is considered to be serious, unless more detailed cases are set out in the European Commission's implementing legislation.

IV CHAPTER 1

EXCHANGE OF INFORMATION AND INTERINSTITUTIONAL COOPERATION

19 Article 1. Cybersecurity Information System

1. Purpose of the Cybersecurity Information System:

1) to register the objects in the Cybersecurity Entity Register and to manage their data;

2) to process data collected by technical cybersecurity measures in order to prevent and manage cyber incidents;

3) processing data related to the monitoring of the implementation of cybersecurity risk management measures;

4) maintain data on cybersecurity actors, other bodies and entities entrusted with the responsibility for managing cyber incidents in the event of an emergency in cyberspace;

5) exchange with the users of the Cybersecurity Information System data related to cyber incidents, cyber threats, near misses, as well as other information related to cybersecurity;

6) maintain and make publicly available data on mandatory orders to block a domain name identifying a website;

7) provide cybersecurity services and tools, including training and exercise services and tools.

2. The operator and data manager of the Cybersecurity Information System is the Ministry of Defence and the administrator and data manager is the National Cybersecurity Centre.

3. Users of the Cybersecurity Information System are entities that meet the requirements specified in the Cybersecurity Information System Regulations. The authorities issuing the instructions referred to in paragraph 1(6) and the cybersecurity entities implementing them shall be obliged to use the part of the Cybersecurity Information System which processes data on mandatory instructions to block a domain name identifying a website, irrespective of the cybersecurity entity's eligibility to the requirements referred to in the Cybersecurity Information System Regulations.

4. Cybersecurity actors have the right to become users of the Cybersecurity Information System through the implementation of reciprocal cybersecurity information sharing agreements. Irrespective of whether the Cybersecurity Information System is used, cybersecurity actors are required to notify the National Cyber Security Centre of

the conclusion of such agreements, as well as the withdrawal from such agreements, within 20 working days from the date of the occurrence of these circumstances.

5. The data of the Cybersecurity Information System shall be confidential and shall be provided to only:

1) Users of the Cybersecurity Information System insofar as it relates to it to the networks and information systems operated and/or maintained by the Cyber Security Information System;

2) the National Cyber Security Centre in carrying out the function set out in Article 7(2)(12) of this Law;

3) managing and/or investigating cyber incidents to the extent necessary for the performance of the functions of the Authority set out in Article 20(1) of this Law;

4) the identification and registration of cybersecurity entities in the Cybersecurity Information System for the performance of the functions of the Authority as laid down in Article 13 of this Law;

5) the publication of data on mandatory orders to block a domain name, identifying a website;

6) for the performance by the police of the function laid down in Article 10(1)(1) of this Law;

7) where the right to receive these data is provided for in the law or its implementing legislation.

20 Article. Inter-institutional cooperation

1. The authorities formulating and implementing cybersecurity policy shall cooperate with each other and with other public authorities, including the Communications Regulatory Authority, the competent authorities in accordance with Regulation (EU) No 910/2014 and Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital resilience in 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, as well as the National Crisis Management Centre, for the purposes set out in this Law, including the exchange of information and data on cyber incidents, cyber threats, and near-misses, as well as the transfer of information pursuant to paragraph 2 of this Article.

2. National Cyber Security Centre:

1) shall inform the National Crisis Management Centre no later than within 20 working days from the date of adoption of the decision to apply the enforcement measure referred to in Article 28(1) of this Law, if the enforcement measure is applied in order to ensure that the material entity complies with the requirements of this Law;

2) no later than 20 working days from the date of adoption of the decision to apply the enforcement measure referred to in Article 28(1) of this Law, inform the following thereof

the competent authority in accordance with Regulation (EU) 2022/2554, where the enforcement measure is applied to ensure that a material entity designated as a critical third country information and communication technology service provider in accordance with Article 31 of Regulation (EU) 2022/2554 complies with the requirements of this Law;

3) provide technical and other advice and assistance to the competent authority in accordance with Regulation (EU) 2022/2554 and have the right to enter into a cooperation agreement referred to in Article 47(3) of Regulation (EU) 2022/2554 with the competent authority in accordance with Regulation (EU) 2022/2554;

4) upon discovering that a material or important subject may be in danger of committing a personal data breach, shall inform the State Data Protection Inspectorate without undue delay, but at the latest within 36 hours from the moment of discovering this circumstance, indicating the information available on the circumstances referred to in Article 33(3) of Regulation (EU) 2016/679;

5) cooperate with the Communications Regulatory Authority in the area of cybersecurity audits of the trust service provider, including informing the Communications Regulatory Authority immediately, but at the latest within 24 hours, of the receipt of reports of cyber incidents by the trust service provider;

6) no later than within 20 working days from the date of adoption of the decision to apply the enforcement measure referred to in Article 28(1) of this Law, it shall inform the competent authority of another Member State of the European Union responsible for the enforcement of the cybersecurity requirements, if the cybersecurity entity is providing services or if its network and information systems are located in that Member State of the European Union;

7) cooperate with the competent authorities of other Member States of the European Union responsible for the enforcement of cybersecurity requirements where the cybersecurity entity provides services in more than one Member State of the European Union or provides services in one or more Member States of the European Union, and its network and information systems are located in one or more other Member States of the European Union, in the context of requests for mutual assistance in the procedure laid down in Article 21 of this Law;

8) consult the European Central Bank before carrying out the inspections referred to in Article 26 of this Law or applying the enforcement measures referred to in Article 28 of this Law in respect of the Bank of Lithuania.

21 Article 2. Mutual assistance

1. The National Cyber Security Centre shall, upon receipt of a request for mutual assistance from a competent authority of another Member State of the European Union, carry out the inspection and/or enforcement of a cyber security entity referred to in Articles 26 and 28 of this Law

u "nsurveillance measures, as well as any other action requested and authorised by this ţLaw. When providing mutual assistance to an entity referred to in Article 12(1)(3) of this Law, whose head office is located outside the Republic of Lithuania, the National Cyber Security Centre may not undertake any more actions than those specified in the mutual assistance request.

2. The National Cyber Security Centre may reject a mutual assistance request from a competent authority of another Member State of the European Union only in cases where:

1) The National Cyber Security Centre does not have the competence to provide the requested assistance;

2) the assistance requested is not proportionate to the human or financial resources available to the National Cyber Security Centre;

3) the request relates to information or involves activities the disclosure or performance of which would be contrary to the interests of the national security, public security or defence of the Republic of Lithuania.

3. If the National Cyber Security Centre is not able to execute a mutual assistance request within its competence, but determines that the request should be executed by another State authority, it shall not examine the request, shall forward it to the other State authority and shall inform the competent authority of the other State that submitted the request.

4. The National Cyber Security Centre, if it is unable to comply with a request for mutual assistance from a competent authority of another Member State of the European Union, shall inform the latter, stating the reasons for its inability to comply with the request, and, in the case of a request from another Member State of the European Union, shall consult the European Commission and/or the Cyber Security Agency of the European Union before rejecting such request.

22 Article 2. Information processed in the framework of interinstitutional cooperation

protection

1. The cybersecurity policy-making and implementing authorities shall have the right to exchange information obtained for the purposes of this Law, including personal data and confidential information, with each other, with other public authorities, with NATO and European Union institutions and with international organisations only to the extent necessary for the exercise of the functions of this authority in accordance with its competence, taking into account the purpose of the exchange of information and proportionality.

2. The cybersecurity policy-making and implementing authorities shall protect classified information, personal security and commercial interests, as well as the confidentiality of the information provided, when handling information received for the purposes of this Law. The information referred to in this paragraph shall be provided only in cases where the right to receive this information is established by law or by the jq

implementing regulatory acts.

3. The cybersecurity policy-making and implementing authorities shall process personal data processed for the purposes of this Law in accordance with the Law on the Legal Protection of Personal Data of the Republic of Lithuania, Regulation (EU) 2016/679 and the Law on the Legal Protection of Personal Data of the Republic of Lithuania processed for the purposes of prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, or for the purposes of national security or defence.

23 Art. Cybersecurity community of competence

1. Legal entities registered in the Republic of Lithuania with at least one of the areas of cybersecurity expertise referred to in Article 8(3) of Regulation (EU) 2021/887, which are able to contribute to the mission of the European Cybersecurity Industry, Technology and Research Centre of Excellence and the National Co-ordination Centre Network, shall have the right to become a member of the Community of Cybersecurity Expertise, which is to be set up on the basis of Article 8 of Regulation (EU) 2021/887 (hereafter referred to as the 'Community'). Persons of national security interest may not be members of the Community.

2. The registration of legal entities as members of the Communities shall be carried out by the National Focal Point designated in accordance with the procedure laid down in Article 6 of Regulation (EU) 2021/587, following an assessment which confirms that the legal entities concerned meet the requirements set out in Article śio(1). The National Coordination Centre shall not register legal persons as members of the Community if they constitute a threat to national security interests. Information on whether these persons may pose a threat to national security interests shall be provided, on the request of the National Coordination Centre, by the authorities referred to in Article 12(7) of the Law on the Protection of Objects Important to National Security, in accordance with the criteria for assessing the conformity of investors with the law on the protection of objects important to national security. The mentioned authorities shall submit their conclusions on the investor's compliance with the national security interests no later than within 15 working days from the date of receipt of the application by the National Cyber Security Centre. If the authorities do not submit an opinion within the time limit specified in the preceding paragraph, it shall be deemed that the authorities have no information on the threat to national security interests of the legal entity.

3. A legal entity registered in the Republic of Lithuania wishing to become a member of the Community (hereinafter referred to as the "applicant") shall submit an application to the National Coordination Centre stating:

1) the name of the legal entity, the legal entity code, the address of the registered office and contact details (e-mail address, contact number);

2) the contact details of the representative of the legal entity (e-mail address, contact number);

3) a confirmation that the applicant is not subject to one of the provisions of Regulation (EU, Euratom) 2018/1046 of the European Parliament and of the Council of 18 July 2018 on the financial rules applicable to the general budget of the Union and amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU)
No 1316/2013, (EU) No 223/2014, (EU) No 283/2014 and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012, as amended, the exclusion criterion set out in Article 136;

4) information on the applicant's cybersecurity expertise in at least one of the areas referred to in Article 8(3) of Regulation (EU) 2021/887.

4. The national coordination centre shall evaluate the applicant and the information provided by the applicant, as well as the information provided by the competent authorities in accordance with paragraph 2 of this Article, and shall take a decision within 2 months from the receipt of the applicant's request:

(l) to register the applicant as a member of the Community;

2) refuse to register the applicant as a member of the Society.

5. The National Coordination Centre shall expel a member of the Community from the Community if:

1) The member of the Community submits a request for his/her exclusion from the membership of the Community;

2) A member of the Community shall no longer comply with the provisions of paragraph 1 of this Article.

6. The decision to expel a member of the Community shall be taken by the National Coordination Centre within 10 working days from the date of receipt of the request of the member of the Community to be expelled, or from the moment when other circumstances referred to in paragraph 5(2) of the present Article come to light.

7. If the National Coordination Centre refuses to register an applicant as a member of the Community, the applicant shall have the right to reapply for membership of the Community. The National Coordination Centre shall have the right not to examine the resubmitted application if:

1) 2 months have not elapsed since the earlier decision to refuse to register the applicant as a member of the Community; and

2) the factual circumstances which were the basis for the decision to refuse to register the applicant as a member of the Community have not changed.

8. The applicant shall have the right to appeal to the court against the decisions of the National Coordination Centre referred to in paragraphs 4(2), 5(2) and 7 of this Article, in accordance with the procedure laid down by the Law on Administrative Procedure.

24 Article 2. Voluntary notification

1. Entities which are not obliged to report cyber incidents, cyber threats, near misses and/or cyber incident management measures under Article 18(1) of this Law shall have the right to report them voluntarily

to the National Cyber Security Centre. The National Cyber Security Centre shall handle such notifications in accordance with the procedures set out in the National Cyber Incident Management Plan.

2. The voluntary reporting of a cyber incident, cyber threat, near miss and/or cyber incident management measures shall not impose a reporting obligation on the entity.

25 Article 3. Search and disclosure of Spragq

1. The search for and disclosure of a vulnerability shall be considered lawful and shall not expose the entity that performed such actions to legal liability only in cases where the search for a vulnerability is performed on networks and information systems owned and operated by the cybersecurity entity, in accordance with the provisions of paragraph 2 of this Article, the description of the national procedure for disclosure of vulnerabilities approved by the Minister of National Defence and/or the description of the procedure for disclosure of vulnerabilities established by the cybersecurity entity, as well as with the restriction set forth in paragraph 6 of this Article.

2. The following limitations shall be respected in the search for vulnerabilities:

1) the operation, functionality, service and data availability or integrity of the network and the information system shall not be disrupted or altered;

2) once the existence of a vulnerability has been verified, the vulnerability search shall be terminated in relation to the discovered vulnerability

the vulnerability;

3) the entity that carried out the search for the vulnerability shall, no later than 24 hours after the search for the vulnerability within 24 hours of the start of the search (every 24 hours if the search is continued beyond 24 hours), the entity shall prepare the information on the results of the search for the gap, with the content specified in the National Gap Disclosure Procedures or the cybersecurity entity's Gap Disclosure Procedures, and shall provide it to the National Cyber Security Centre, in accordance with the procedures set out in the National Gap Disclosure Procedures, and/or to the cybersecurity entity, the network and information system of which the vulnerability has been searched, in accordance with the procedures set out in the description of the vulnerability disclosure procedures established by that cybersecurity entity;

4) not unnecessarily seek more than is necessary to validate, monitor, record, intercept, acquire, retain, disclose, copy, modify, alter, destroy, corrupt, remove, or obliterate the data controlled and/or maintained by the cybersecurity entity;

5) the disclosure of the vulnerability does not involve the use of observed, recorded, intercepted, disclosed personal data;

6) no attempt is made to disable passwords, no illegally obtained passwords are used, and no manipulation of the cybersecurity entity's employees or other entities with access to non-public information relevant to the search for the vulnerability occurs;

7) not sharing information on the discovery of a vulnerability, except for the purposes of point 3 of this paragraph and this

(b) in the cases referred to in paragraph 3(2), (3), (3), (4), (5) and (6), as well as where the information on the discovered vulnerability is registered in the European vulnerability database.

3. The entity that has collected information about the vulnerability shall have the right to submit the information anonymously to the National Cyber Security Centre, while preserving the information on the submission of the results of the search for the vulnerability as specified in the national vulnerability disclosure procedure. The National Cyber Security Centre shall ensure the anonymity of the entity reporting the vulnerability. The entity that has collected and anonymised the information referred to in this paragraph regarding the submission of the vulnerability search results shall retain the information on the submission of the vulnerability search results for a period of 12 years from the date of the submission of the notification to the National Cybersecurity Centre.

4. The procedure for disclosure of the vulnerability to the National Cyber Security Centre, the content of the information on vulnerabilities to be provided to the National Cyber Security Centre, the procedure for setting the time limit for disclosure of the information on the discovered vulnerability to entities other than those referred to in point 3 of paragraph 2 of this Article for a shorter period of less than 90 calendar days shall be set out in the description of the national procedure on vulnerability recovery.

5. A cybersecurity entity shall have the right to establish procedures for the disclosure of vulnerabilities in networks and information systems under its control and/or management, and to impose or refuse to impose restrictions on the search for vulnerabilities other than those provided for in paragraph 2 of this Article. The limitations on the search for vulnerabilities set out in the description of the procedures for disclosure of vulnerabilities established by the cybersecurity entity may not be stricter than those set out in paragraph 2 of this Article. The description of the procedures for disclosure of vulnerabilities established by the cybersecurity entity may not establish procedures for the submission of information on vulnerabilities to the National Cyber Security Centre and may not provide for exceptions to the regulation set out in paragraph 6 of this Article.

6. An entity that has identified a vulnerability shall, subject to the restriction referred to in paragraph 1 of this Article, have the right to disclose the information on the identified vulnerability, up to a maximum of the information provided to the National Cyber Security Centre and/or the Cyber Security Entity, to entities other than those referred to in paragraph 2(3) of this Article, not earlier than 90 calendar days after the date of the provision of the information on the vulnerability to the National Cyber Security Centre and/or Cyber Security Entity. The National Cyber Security Centre, after assessing the complexity of the vulnerability and the possibility of its correction, shall have the right to set a shorter time limit for the disclosure of the information on the discovered vulnerability to entities other than those referred to in point 3 of paragraph (2) of this Article, however, not shorter than 3 calendar days, in accordance with the procedure set out in the description of the procedure for disclosure of the national vulnerability.

V CHAPTER
INSPECTIONS AND ENFORCEMENT MEASURES

26 Art. Inspections of cybersecurity entitiesq

1. The National Cyber Security Centre shall carry out inspections of the compliance of the cyber security entity with the requirements of this Law, except for those set out in Chapters VI and VII of this Law.

2. The National Cyber Security Centre shall have the right to initiate the inspection of a cyber security entity referred to in paragraph 1 of this Article on any matter related to the requirements of this Law imposed on cyber security entities and the non-compliance with which shall be considered as a violation, on its own initiative, on the basis of a complaint, or on the basis of any other source, except for cases referred to in paragraph 3 of this Article.

3. The inspections referred to in paragraph 1 of this Article shall be carried out on a significant entity only upon receipt of data or information that the significant entity is suspected of having committed a breach of the requirements of this Law.

4. The inspections referred to in paragraph 1 of this Article shall be carried out in accordance with the procedures laid down in Article 27 of this Law and the National Cyber Security Centre. The description of the procedure for conducting the inspection, to be approved by the National Cybersecurity Centre, shall include the procedure for prioritising the cybersecurity risk after the inspection.

27 Article 3. General grounds for conducting a cybersecurity entityq review

1. An inspection shall be carried out as soon as possible, but at the latest within 4 months from the date of receipt of the complaint or the date of the decision of the Director of the National Cyber Security Centre or his/her delegate to carry out an inspection on his/her own initiative or on the basis of another source.

2. Taking into account the complexity and scope of the inspection, the activities of the cybersecurity entity

In the case of a violation of the requirements of the National Cyber Security Centre, new circumstances that have arisen during the course of the investigation or other objective reasons, the time limit set out in paragraph 1 of this Article may be extended by a decision of the Director of the National Cyber Security Centre, for a period not exceeding 2 months. The total time limit for carrying out an inspection may not exceed 6 months from the date of receipt of the complaint or from the date of the decision to carry out an inspection on its own initiative or on the basis of another source. The National Cyber Security Centre shall notify the extension of the time limit for the inspection and the reasons for which the time limit has been extended

notify the inspected entity of the extension of the time limit referred to in paragraph 1 of this Article without delay, but at the latest before the expiry of the time limit.

3. In carrying out the inspections referred to in Article 26(1) of this Law, the National Cyber Security Centre shall have the right:

1) Enter the premises of the cybersecurity entity to be inspected (including those rented or used for other purposes), for a period of up to 30 calendar days, to take copies and transcripts of documents, copies of data and other items necessary to carry out the inspection. Access to the premises of the legal entity (including those rented or used for other purposes) shall be allowed only during the working hours of the legal entity, upon presentation of a tamybinț certificate and a document certifying the decision of the National Cyber Security Centre to carry out the inspection or any other authorisation granted by the head of the National Cyber Security Centre. Access to premises belonging to a natural person (including premises rented or used for other purposes) is subject to the production of a court order authorising access to premises belonging to a natural person;

2) instruct the cybersecurity entities subject to inspection to carry out, at their own expense, an independent targeted cybersecurity audit of the network and information system or of the activity or service provided by them, and to provide the results of that audit if the results of the cybersecurity risk analysis indicate a high level of risk;

3) issue instructions to provide all necessary information, copies and extracts of documents, copies of data, as well as access to all data and documents necessary for the compliance of the cybersecurity entity's network and information system with Article 14 of this Law
1, including the results of a cybersecurity audit showing the compliance of the network and information system with the requirements referred to in paragraph 1;

4) instruct entities with information relevant to the inspections to provide oral and written explanations, and require them to appear at the premises of the National Cyber Security Centre to provide explanations;

5) use, at its own expense, an independent, impartial and impartial entity meeting the criteria of good repute laid down in the Civil Service Law and possessing the necessary qualifications and experience;

6) to contract with audit firms, other entities whose services will be used by the National Cyber Security Centre in the course of the audit. The contracts referred to in this point shall be subject to the requirements referred to in Article 7(3) of this Law;

7) to use all the information available to the National Cyber Security Centre, including information obtained in the course of other inspections;

8) exercise the other rights conferred by the Law.

4. When issuing the instruction provided for in paragraph 3(3) of this Article, the National Cyber Security Centre shall specify the purpose of the request, the grounds for the request and the precise nature of the information requested.

5. The National Cyber Security Centre shall take at least one of the following decisions upon completion of the inspection:

1) Determine that no violation has been found;

2) upon finding an infringement of this Law, apply the enforcement measures referred to in Article 28 of this Law.

6. In the event of a breach of this Law, the enforcement measures referred to in Article 28 of this Law, other than those referred to in Article 28(1)(9) to (11), may be applied after the completion of the inspection, taking into account the complexity of the inspection, the scale of the inspection, the cybersecurity entity's failure to comply w i t h the requirements of the National Cyber Security Centre, the new circumstances that have emerged in the course of the inspection, or any other objective reasons.

7. Before deciding to impose the enforcement measure(s) referred to in Article 28(1) of this Law, the National Cyber Security Centre must inform the cyber security entity to which the enforcement measure(s) is (are) to be applied, providing essential information on the provisions of the legal act and the factual findings, which constitute the grounds for the enforcement measure(s), and to set a deadline of at least 20 working days from the date of notification to provide explanations, unless this would prevent immediate action to prevent or respond to a cyber incident. When imposing the measures of sanctions referred to in Article 28(1)(9) to (11) of this Law, the deadline of 20 working days for the submission of explanations referred to in this paragraph shall be fixed.

28 Article 28. Enforcement measures

1. The National Cyber Security Centre shall apply one or more enforcement measures in the event of a breach of this Law being detected during an inspection referred to in Article 26(1) of this Law:

1) issuing notifications that cybersecurity entities are in breach of the requirements laid down in this Law;

2) instruct the relevant entities on the measures to be taken to prevent or manage a cyber incident and the timing of the implementation of such measures and the timing of the submission of a report on the implementation of such measures, and instruct the relevant entities to remedy the identified deficiencies or to correct the breaches of the requirements laid down in this ţlaw;

3) instruct cybersecurity entities to cease and desist from repeating acts that violate the requirements laid down in this Law;

4) instruct cybersecurity entities to ensure, within a specified period of time, that the cybersecurity risk management tools used by them comply with the legislation referred to in Article 14(1) of this Law or that they comply with the obligation to report cyber incidents laid down in Article 18(1) of this Law;

5) instruct cybersecurity entities to inform the entities to which they provide services or for which they carry out relevant activities and which may be affected by a major cyber threat of the nature of the threat, as well as of any possible action that may be taken by those entities in response to that threat;

6) instruct cybersecurity entities to implement the recommendations of the cybersecurity audit within a reasonable timeframe;

7) appoint a monitoring officer, who shall be entrusted with clearly defined tasks within a specified period of time, to monitor the compliance of material entities with the requirements laid down in Articles 14 and 18 of this Law;

8) instruct cybersecurity entities to publicise aspects of a breach of this Law at the appropriate time;

9) impose a fine on cybersecurity entities in accordance with the procedure laid down in Articles 30 and 31 of this Law, in addition to any of the measures referred to in points 1 to 8, 10 and 11 of this paragraph;

10) initiate the suspension of the right to carry out part or all of the activities of the essential entity or the right to provide services, as provided for in Article 32 of this Law;

11) initiate the suspension of the head of a substantial entity, other than the head of a public administration entity appointed by a decision of the Seimas, the Government and the President of the Republic of Lithuania, as provided for in Article 33 of this Law.

2. The imposition of an enforcement measure shall not exempt the cybersecurity entity from the performance of the obligation for the non-performance of which the enforcement measure was imposed. The application of an enforcement measure to legal persons shall not exempt their directors and employees from civil, administrative or criminal liability under the law.

3. In applying any of the enforcement measures referred to in paragraph 1 of this Article, the National Cyber Security Centre shall take into account the circumstances of each individual case, including the following:

1) the mitigating circumstances set out in paragraph 4 of this Article, the aggravating circumstances set out in paragraph 5 of this Article, and the seriousness of the infringement referred to in Article 29 of this Law;

2) the duration of the infringement;

3) previous infringements of this Law committed by the entity in the last 2 years;

4) the material or non-material damage caused, which shall be assessed in terms of financial or economic loss, the impact on other services and the number of users affected, the compensation for the damage or the reversal of the negative effects caused;

5) the measures which the entity will take to prevent or mitigate material or non-material damage;

6) compliance with an approved code of conduct or an approved certification mechanism;

7) cooperation with the National Cyber Security Centre;

8) the extent of the breach;

9) whether the entity that committed the breach acted intentionally or recklessly.

4. The mitigating circumstances are:

1) the subject has voluntarily prevented material or non-material damage;

2) the subject has made reparation for the damage caused;

3) the subject has admitted the infringement and has assisted the National Cyber Security Centre during the inspection;

4) the entity voluntarily ends the infringement.

5. The aggravating circumstances are:

1) the infringement is repeated. An infringement shall be deemed to have been committed repeatedly if the entity suspected of committing the infringement has committed such an infringement within the last 12 months following the date of entry into force of the decision imposing the enforcement measure. In the event of a repeat offence, the time limit laid down in this paragraph shall be restarted;

2) a serious infringement within the meaning of Article 29 of this Law has been committed

paragraph 2;

3) the subject has failed to remedy the trükumq in accordance with the information provided by the National Cyber Security Centre

instructions;

4) the entity has obstructed the activities of a cybersecurity audit or monitoring officer, which the National Cybersecurity Centre was obliged to carry out following the discovery of a breach;

5) the entity has provided incorrect information in relation to the requirements of this Law;

6) the entity has committed or continued an infringement despite the fact that the National Cyber Security Centre had drawn attention to the infringement or operational deficiencies.

6. The enforcement actions referred to in paragraph 1 of this Article shall be applied in accordance with the procedure for the application of enforcement measures established by the Government.

7. A decision on the imposition of an enforcement measure may be taken if no more than 2 years have elapsed from the date of the infringement, or, in the case of a continuing infringement, if no more than 2 years have elapsed from the date on which the infringement was discovered.

29 Article 2. Infringements subject to enforcement measures

1. Infringements shall be deemed to be a failure to comply with the requirements laid down in this Law and its implementing legal acts, or an obstruction of the authorities referred to in Article 4(2) and (3) of this Law, including the entities they designate, in the performance of the functions assigned to them. Infringements shall be classified as ¡ serious, moderate and minor.

2. Infringements of the requirements laid down in Articles 14(1), 18(1)(1) of this Law shall be regarded as serious infringements.

3. Infringements of the requirements laid down in Article 7(2)(6) and (7), Article 14(6) and (8) and Article 15(1), (2) and (3) of this Law, or the obstruction of the authorities in the performance of the functions assigned to them by Article 27(3) of this Law, and of the requirements laid down in Article 17 of this Law, shall be regarded as medium seriousness, provided that they have been committed by the entities providing top-level domain name registration services.

4. The infringements referred to in Article 14(3) and (7), Article 18(1)(2) and Article 19(4) of this Law, as well as the infringements referred to in Article 17 of this Law shall be considered to be minor infringements, if committed by the entities providing domain name registration services.

30 Article 2. Penalties

1. Fines shall be imposed by the Head of the National Cyber Security Centre or his/her delegate in accordance with the procedure for the application of enforcement measures to essential and critical entities established by the Government.

2. The maximum fines shall be imposed for the infringements referred to in Article 29 of this Law:

1) for a material entity, up to EUR 10 000 000 or up to 2 per cent of the total annual worldwide turnover of the legal person during the preceding financial period, whichever is the higher amount;

2) for a significant entity, up to EUR 7 000 000 or up to 1,4 per cent of the legal person's total annual worldwide turnover for the preceding financial period, whichever is the greater amount;

3) for a budget institution which is a substantial entity - up to 1 per cent of the budget of the budget institution for the current year and the amount of the annual revenue of the budget institution for the previous year, but not exceeding EUR 60 000;

4) for a budgetary institution which is a significant entity - up to 0,5 per cent of the budget of the budgetary institution for the current year and of the amount of the bendrijjq's annual revenue for the previous year, but not more than EUR 30 000.

3. The following fines shall be imposed:

1) up to 100 per cent of the maximum fine laid down in paragraph 2 of this Article, if the infringement is considered to be a serious infringement pursuant to Article 29(2) of this Law;

2) up to 50 per cent of the maximum fine laid down in paragraph 2 of this Article, if the infringement is considered to be of medium gravity in accordance with Article 29(3) of this Law;

3) up to 10 per cent of the maximum fine laid down in paragraph 2 of this Article, if the infringement is considered to be a minor offence pursuant to Article 29(4) of this Law.

4. The amount of the fine to be fixed shall be effective, proportionate to the infringement committed and shall act as a deterrent against future infringements. The amount of the fine shall take into account the circumstances referred to in Article 28(3) to (5), with the exception of the circumstance referred to in Article 28(5)(2).

31 Article 28. Procedure for imposing fines

1. The National Cyber Security Centre shall, as a general rule, examine the question of imposing a fine in accordance with a written procedure, on the basis of the explanations submitted to it in accordance with the procedure laid down in Article 27(7) of this Law. No hearing shall be held when the imposition of a fine is considered in accordance with the written procedure.

2. The National Cyber Security Centre may, at the request of the cyber security entity to be fined or on its own initiative, due to the complexity of the circumstances or any other relevant circumstance, decide to consider the imposition of a fine by oral procedure, where it is expedient to hear oral explanations from the cyber security entity suspected of having committed the infringement, or otherwise where the imposition of a fine may be better considered by the oral procedure. Where it is decided to consider the imposition of a fine orally, the cybersecurity entity to be fined and other interested parties shall be notified by e-mail of the place, date and time of the hearing at which the imposition of the fine is to be considered at the latest 10 working days prior to the date of the hearing.

3. The cybersecurity entity that committed the infringement and is to be fined, and any other entity whose participation is necessary for the proper consideration of the imposition of the fine, may attend and provide explanations at the meeting at which the imposition of the fine is to be considered.

4. The absence of the cybersecurity entity to be fined or its representative shall not prevent the consideration of the imposition of a fine, provided that the entity has been duly notified of the hearing and does not provide evidence that it is unable to attend for important reasons.

5. The hearing on the imposition of a fine shall be public, except where the National Cyber Security Centre, on its own initiative or at the request of the cyber security entity subject to a fine and/or another interested entity, decides to discuss the imposition of a fine in a closed session in order to protect state, official, professional, commercial secrets or other secrets protected by law, or to safeguard the rights of the entity with regard to the inviolability of its privacy and/or the protection of its personal dataq .

6. The hearing at which the imposition of a fine is considered shall be held in Lithuanian. Persons who do not speak the official language shall be guaranteed the right to use the services of an interpreter.

7. An audio recording shall be made of the hearing at which the imposition of the fine is being considered. It shall be taken as a record of the hearing.

8. Where the imposition of a fine is considered in a written procedure, the National Cyber Security Centre shall take a decision on the imposition of a fine within 20 working days from the expiry of the time limit for the submission of explanations set out in Article 27(7) of this Law. If the imposition of a fine is discussed in an oral procedure, the National Cyber Security Centre shall adopt a decision on the imposition of a fine within 20 working days from the date of the hearing. The National Cyber Security Centre shall send a copy of the decision to impose a fine to the entity in respect of which the decision has been taken and, if the fine is imposed following an investigation initiated on the basis of a complaint received, to the entity that lodged the complaint, no later than 3 working days from the date of adoption.

9. The decision of the National Cyber Security Centre to impose a fine must be reasoned. It shall contain the information referred to in Article 10(5) of the Public Service Act, including:

1) details of the essential or relevant subject on which the decision is taken;

2) the irregularities, if any, and the circumstances thereof;

3) the evidence gathered and the assessment of jq;

4) explanations, if any, from the cybersecurity entity alleged to have committed the breach and from other e n t i t i e s , and jq assessment;

5) the decision taken to impose or not to impose a fine.

10. No fine shall be imposed if the cybersecurity entity has already been fined for the same breach in accordance with Article 58(2)(i) of Regulation (EU) 2016/679.

11. The decision of the National Cyber Security Centre to impose a fine may be appealed to the court in accordance with the procedure laid down in the Lawon Administrative Procedure.

12. The decision of the National Cyber Security Centre on the imposition of a fine shall be

be executed at the latest within 3 months from the date on which it was served on the entity on which the fine was imposed. In the event of an appeal against the decision of the National Cyber Security Centre on the imposition of a fine, it shall be enforced at the latest within 3 months from the date of the entry into force of the judgment declaring the imposition of the fine justified. The fine shall be paid to the State budget.

13. The decision of the National Cyber Security Centre on the imposition of a fine shall be an enforceable document and shall be executed in accordance with the procedure laid down in the Code of Civil Procedure. It may be submitted for execution no later than 3 years from the date of its adoption.

32 Article. Suspension of the right to carry on part or all of the activities of a substantial entity or the right to provide services

1. The District Court of General Jurisdiction, upon receipt of a request from the National Cyber Security Centre, shall have the right to suspend, by a ruling, the right to engage in part or all of the activities of a substantial entity or the right to provide services, if it is established that the application of the enforcement measures referred to in Article 28(1)(1)(4) and (6) of this Law is ineffective. Suspension of the right to carry on part or all of the activities of a substantial body or of the right to provide services may only be imposed for the serious infringements referred to in Article 29(2) of this Law.

2. The National Cyber Security Centre shall, before requesting the District Court of General Jurisdiction to suspend part or all of the activities or the provision of services of a material entity on the grounds referred to in paragraph 1 of this Article, inform the material entity of the provisions of the law and the factual findings, by providing the material information, which constitute the grounds for the suspension of part or all of the essential entity's activities or of the right to provide services, and to set a time limit, which may not be less than 10 working days from the date of notification, by which the essential entity must take the necessary steps to remedy the deficiencies identified or to comply with the requirements. The National Cyber Security Centre shall have the right to refer the matter to a district court of general jurisdiction on the grounds set out in paragraph 1 only after the expiry of the time limit set by the National Cyber Security Centre and the failure of the material entity to take the prescribed action.

3. The request of the National Cyber Security Centre to the District Court of General Jurisdiction for the right to suspend part or all of the activities or services of the essential entity states:

1) the activities or part of the activities or services of the essential entity for which the suspension is sought;

2) the circumstances demonstrating that the application of the security measure referred to in Article 28(1)(1)(4) and (6) of this Law is ineffective;

3) circumstances showing that the essential entity has been given a time limit to remedy the deficiencies or to comply with the requirements and that the essential entity has failed to take the prescribed action;

4) explanations, if any, from the substantial entity whose right to carry out part or all of the activities or to provide services is requested to be suspended.

4. An order to suspend the right to carry on part or all of the activities or to provide services of a substantial entity shall oblige the substantial entity to suspend all or part of the commercial, business, financial, professional activities specified in its constituent documents and to close all or part of the establishments connected with those activities or parts of them. The order shall specify the period of suspension of the activities of the substantial entity, which may not exceed 4 months. If the application of the security measures referred to in Article 28(1)(1)(4) and (6) of this Law is still ineffective, upon the request of the National Cyber Security Centre, the time limit may be extended by order of a district court of general jurisdiction, but not for more than 2 months. The number of extensions shall not be limited, but in all cases the suspension of the right to carry out part or all of the activities of the essential entity or the right to provide services may not last longer than is necessary to ensure compliance with the provisions of this Law.

5. An order suspending the right to engage in some or all of the activities of the essential entity or the right to provide services shall be sent without delay to the bailiff for execution, to the National Cyber Security Centre and, where appropriate, to the information system operator of the relevant public register.

6. The order suspending the right to engage in part or all of the activities carried out by the essential entity, or the right to provide services, shall be notified to the essential entity or its representative in accordance with the procedure laid down by the Code of Civil Procedure.

7. The substantial entity may appeal against the order of the district court of general jurisdiction suspending the right to engage in part or all of the activity or the right to provide services, as well as against the order extending the period of application of this measure, to a court of higher instance within 7 working days from the date of service of the order. The order made by that court shall be final and non-appealable.

8. The National Cyber Security Centre shall, upon receipt of a reasoned request from a material entity whose activities or services have been suspended in whole or in part and upon finding that the suspension of the material entity is no longer necessary, apply to a district court of general jurisdiction for lifting of the suspension no later than 7 working days from the date of receipt of the request. The district court of general jurisdiction shall

the court shall lift the suspension of the activity or provision of services of a substantial entity when the measure is no longer necessary and the National Cyber Security Centre requests the lifting of the suspension.

9. The National Cyber Security Centre shall publish on its website the information on the material entity that has been temporarily suspended from some or all of its activities or from the provision of services for the entire duration of this enforcement measure.

33 Article 2. Suspension of the head of an essential entity

1. The District Court of General Jurisdiction, upon receipt of a request from the National Cyber Security Centre to suspend the head of a material entity, shall have the power by order to suspend the head of a material entity if it is established that the application of the enforcement measures referred to in Article 28(1)(1)(4) and (6) of the present Law is ineffective. The suspension of the head of the material entity may only be imposed for a serious breach referred to in Article 29(2) of this Law.

2. The National Cyber Security Centre shall, before requesting the district court of general jurisdiction to suspend the head of a material entity on the grounds referred to in paragraph 1 of this Article, inform the material entity by providing essential information on the provisions of the legislation and the factual findings, which constitute the grounds for the suspension of the head of the material entity, and to set a time limit, which shall not be less than 10 working days from the date of notification, within which the material entity shall take the necessary steps to remedy the deficiencies identified or to comply with the requirements. The National Cyber Security Centre shall have the right to apply to the district court of general jurisdiction on the grounds set out in paragraph 1 only after the expiry of the time limit set by the National Cyber Security Centre and the failure of the material entity to take the action specified.

3. The request of the National Cyber Security Centre to the District Court of General Jurisdiction for the suspension of the head of a material entity states:

1) the circumstances showing that the application of the security measure referred to in Article 28(1)(1)(1) to (4) and (6) of this Law is ineffective;

2) circumstances demonstrating that the material entity has been given a time limit to remedy the deficiencies or to comply with the requirements and the material entity has failed to take the prescribed action;

3) explanations, if any, from the head of the material entity whose manager is requested to be suspended.

4. The order suspending the head of the essential entity shall be sent without delay to the j†††† host entity and the National Cyber Security Centre.

5. An order suspending the head of a material entity shall be notified to the head of the material entity or his representative in accordance with the procedure laid down in the Code of Civil Procedure.

6. From the date of publication of the order of the district court of general jurisdiction suspending the manager of the essential entity, the suspended manager of the essential entity shall not be entitled to perform his functions and all decisions taken by him after the date of publication of such order shall be null and void.

7. The suspension of the head of a material entity may not exceed 6 months. If necessary, this measure may be extended for up to 3 months. The number of extensions shall not be limited, but in all cases the suspension may not last longer than is necessary to ensure compliance with the provisions of this Law.

8. An order to suspend the head of a material entity, as well as an order to extend the period of application of this measure, may be appealed by the material entity or the head of the material entity who has been suspended, to a court of higher instance within 7 working days of the date of publication of the order. The order made by that court shall be final and not subject to appeal.

9. The National Cyber Security Centre, upon receipt of a reasoned request from the head of the suspended material entity and upon determining that the suspension of the head of the material entity is no longer necessary, shall, not later than 7 working days from the date of receipt of the request, request the District Court of General Jurisdiction to lift the suspension of the head of the material entity from his/her duties. The district court of general jurisdiction shall revoke the suspension of the head of the essential entity when the measure is no longer necessary and the National Cyber Security Centre requests the revocation of the suspension of the head of the essential entity.

10. The National Cyber Security Centre shall publish on its website the information on the material entity whose head has been suspended for the duration of the enforcement measure.

VI CHAPTER 2

POWERS OF THE NATIONAL CYBERSECURITY CERTIFICATION AUTHORITY

34 Article 1. National cybersecurity certification authority

1. The National Cyber Security Centre shall exercise the functions of a national cybersecurity certification authority as set out in Regulation (EU) 2019/881 and shall have the powers of a national cybersecurity certification authority.

2. The National Cyber Security Centre shall exercise the functions of a national cybersecurity certification authority:

1) shall have the right to obtain, free of charge, from the conformity assessment body, the holder of the European Cyber Security Certificate, the European Union Conformity Statement Issuing Body, the State and municipal authority and the institution, all the information, copies and transcripts of documents, copies of data, as well as access to all data and documents, necessary for the performance of the functions of the national cyber security certification body;

2) determine the procedures for granting, limiting and suspending, limiting and suspending, revoking, granting, limiting, suspending or revoking additional authorisations for conformity assessment bodies pursuant to Article 60(3) of Regulation (EU) 2019/881} (hereinafter referred to as "additional authorisations") in the cases set out in Article 35 of the present Law;

3) The Public Administration Law shall deal with complaints referred to in Article 58(7)(f) of Regulation (EU) 2019/881 in accordance with the procedure laid down by the Public Administration Law;

4) carry out investigations, in accordance with the procedure laid down in Regulation (EU) 2019/881, Article 36 of this Law and the procedure laid down by the National Cyber Security Centre, on compliance with the provisions of Title III of Regulation (EU) 2019/881 or of the European Cyber Security Certification Scheme, which apply to the certification of the information and communication technology product, information and communication technology service and information and communication technology process;

5) for the purposes of the investigations referred to in point 4 of this paragraph, shall have the right to enter the premises (including those rented or otherwise used) of the Conformity Assessment Body and of the holder of the European Cybersecurity Certificate, and to take for a period of up to 30 calendar days, copies and transcripts of the document, copies of the data, and any other items necessary for the investigations. Access to the premises of the legal entity (including those rented or otherwise used) shall be permitted only during the legal entity's working hours and upon presentation of a certificate to that effect. |Access to premises belonging to a natural person (including those rented or used for other purposes) is subject to the production of a court order dê1 authorising access topremises belonging to a natural person;

6) shall have the right, when carrying out the investigations referred to in point (4) of this paragraph, to receive oral and written explanations from the legal and natural persons to be inspected and to require them to appear at the premises of the national cybersecurity certification authority to give explanations;

7) perform other functions established by the legislation of the Republic of Lithuania in the field of cybersecurity certification.

3. Requests by the National Cyber Security Centre for permission from the court to enter premises belonging to a natural person (including those rented or used on other grounds) shall be dealt with in accordance with the procedure laid down in Chapter XXXIX of the Code of Civil Procedure.

35 **Article 5. Additional {granting, restriction and suspension of authorisations for conformity assessment bodies, additional {revocation of restriction and suspension of authorisations, additional {revocation of authorisations**

1. The granting, limitation and suspension of supplementary ţauthorisations to conformity assessment bodies, the lifting of limitation and suspension of supplementary ţga1iojimq, and the revocation of supplementary ţauthorisations shall be carried out in accordance with the procedure laid down in this Article and in the legislative act referred to in Article 34(2), paragraph 2, point 2, of this ţlaw.

2. Additional powers are granted to conformity assessment bodies to carry out tasks under the European Cybersecurity Certification Schemes when all the following conditions are met:

1) the conformity assessment body meets the requirements set out in the Annex to Regulation (EU) 2019/881 and has a valid accreditation certificate to prove it;

2) the conformity assessment body complies with the specific or additional requirements set out in the European Cybersecurity Certification Scheme.

3. The decision on the granting of additional ţgranting ţgilojimq shall be taken within 30 calendar days of receipt of a duly completed document demonstrating the conformity assessment body's compliance with the conditions referred to in paragraph 2 of this Article.

4. The granting of additional authorisation shall be refused if the National Cyber Security Centre establishes that the conformity assessment body does not comply with the condition referred to in paragraph 2 of this Article.

5. The additional powers shall be limited by a decision of the National Cyber Security Centre specifying the grounds for the limitation of the additional powers, the applicable limitations and, in the case of a limitation of the additional powers on the grounds set out in paragraph 6(2) of this Article, the time limit, which shall not exceed six months from the date of the decision to limit the additional powers and within which the conformity assessment body shall remedy the breaches which led to the limitation of the additional powers.

6. The additional authorisation shall be restricted when at least one of the following conditions is met:

1) the specific or additional requirements set out in the European Cybersecurity Certification Scheme have changed;

2) the National Cyber Security Centre, in the course of its investigation, determines that the conformity assessment body has not complied with the requirements of Regulation (EU) 2019/881 or has breached the requirements set out in the European Cybersecurity Certification Scheme for which the additional powers were granted;

3) the accreditation certificate has been changed in accordance with the procedure laid down by the Law on Conformity Assessment of the Republic of Lithuania.

7. In the event of a decision to restrict the supplementary authorisation, the conformity assessment body shall be prohibited from carrying out the tasks specified in the decision under the European Cybersecurity Certification Scheme for which the supplementary authorisation was granted.

8. The restriction of the supplementary authorisation shall be lifted when the conformity assessment body submits a request no later than 7 months after the date of adoption of the decision to restrict the supplementary authorisation and the National Cyber Security Centre carries out an investigation in accordance with the procedure laid down in Article 36 of this Law and establishes the conditions referred to in paragraph 9 of this Article.

9. Conditions for lifting the restriction on additional ţggajojimq:

1) The conformity assessment body shall comply with the requirements set out in the European Cybersecurity Certification Scheme, provided that the additional ţgranting authority has been restricted on the grounds set out in point 1 of paragraph 6 of this Article;

2) the conformity assessment body has remedied the breaches within the time limit set by the National Cyber Security Centre, which has led to the restriction of the additional authorisation;

3) the scope of accreditation for which the additional authorisations were issued is not narrowed down by amending the accreditation certificate in accordance with the procedure established by the Law on Conformity Assessment of the Republic of Lithuania, if the additional authorisations were limited on the grounds set out in paragraph 6(3) of this Article.

10. Additional privileges shall be suspended by decision of the National Cyber Security Centre. This decision shall specify the grounds for the suspension of the supplementary privileges and, if the supplementary privileges are suspended on the grounds set out in point (2) of this paragraph, the time limit, which may not exceed 6 months, within which the conformity assessment body must remedy the breaches for which the supplementary privileges are suspended, where one or more of the following conditions exist:

1) the conformity assessment body has made a request to the National Cyber Security Centre to suspend the additional powers granted to it for a period specified in the request, which may not exceed 6 months;

2) The National Cyber Security Centre shall, in the course of its investigation, establish that a conformity assessment body whose additional powers have been restricted on the basis set out in paragraph 6(2) of this Article has failed to remedy the breach for which the additional powers have been restricted within the time limit set by the National Cyber Security Centre;

3) the suspension of the accreditation certificate in accordance with the procedure laid down by the Law on Conformity Assessment

the suspension of the validity of the accreditation.

11. The suspension of the additional privileges shall be lifted when the conformity assessment body submits a request not later than within 7 months from the date of adoption of the decision to suspend the additional privileges and the National Cyber Security Centre carries out an investigation in accordance with the procedure laid down in Article 36 of this Law and establishes that:

1) the conformity assessment body meets the requirements set out in the European Cybersecurity Certification Scheme, provided that the additional }authorisation granted to it has been suspended on the grounds set out in point (1) of paragraph 10 of this Article;

2) the conformity assessment body has remedied the breaches within the time limit set by the National Cyber Security Centre for which the additional authorisation was suspended;

3) the suspension of the accreditation certificate has been lifted in accordance with the procedure laid down by the Law on Conformity Assessment, if the additional authorisation has been suspended on the grounds set out in paragraph 10(3) of this Article.

12. The additional authorisations shall be withdrawn by decision of the National Cyber Security Centre when at least one of the following conditions exists:

1) the conformity assessment body has made a request to the National Cyber Security Centre to withdraw the additional authorisation granted to it;

2) the conformity assessment body does not submit a request for the removal of the additional restriction or suspension of the authorisation within the time limits referred to in paragraphs 8 and 11 of this Article;

3) the conformity assessment body has not remedied the breach for which the supplementary privileges were suspended within the time limit set by the National Cyber Security Centre;

4) the conformity assessment body whose supplementary authorisation has been limited or suspended continues to carry out the tasks under the European cybersecurity certification scheme for which the supplementary authorisation has been limited or suspended;

5) The accreditation certificate has been revoked in accordance with the procedure laid down in the Conformity Assessment Act or the scope of accreditation for which the additional authorisation was granted has been narrowed.

36 Article 5. Conduct of an investigation

1. The National Cyber Security Centre shall have the right to initiate an investigation into any matter relating to a possible breach of, or compliance with, Title III of Regulation (EU) 2019/881 or the provisions of the European Cybersecurity Certification Scheme.

2. The grounds for initiating an investigation may include complaints pursuant to Article 58(7)(f) of Regulation (EU) 2019/881, requests from conformity assessment bodies pursuant to Article 35 of this Law and other sources. The National Cyber Security Centre shall also have the right to initiate an investigation on its own initiative.

3. The investigation shall be carried out within the shortest possible period of time, but at the latest within 4 months from the date of receipt of the complaint or request referred to in paragraph 2 of this Article, or the date of the decision to carry out an investigation on the basis of another source referred to in paragraph 2 of this Article.

4. Depending on the complexity of the investigation, the scope of the investigation, the conformity assessment body, the holder of the European Cyber Security Certificate and the issuer of the European Union Statement of Compliance

The time limit set out in paragraph 3 of this Article may be extended by a decision of the National Cyber Security Centre for a period not exceeding 2 months, if new circumstances or other objective reasons have come to light during the investigation. The total time limit for the investigation may not exceed 6 months from the date of receipt of the complaint or request referred to in paragraph 2 of this Article or the date of the decision to conduct an investigation on the basis of another source referred to in paragraph 2 of this Article. The National Cyber Security Centre shall notify the conformity assessment body, the holder of the European Cyber Security Certificate or the issuer of the European Union Statement of Conformity of the extension of the time limit for the investigation and of the reasons for the extension of the time limit without delay, but at the latest by the expiry of the time limit referred to in paragraph 3 of this Article.

5. The National Cyber Security Centre will make at least one of the following decisions after completing its investigation:

1) a finding of no violation;

2) issue instructions and recommendations to the conformity assessment body, the holder of the European Cyber Security Certificate or the issuer of the European Union Declaration of Conformity if the investigation reveals that inappropriate operational methods or practices are being applied;

3) initiate administrative infringement proceedings;

4) invalidate the European Union Statement of Compliance issued in accordance with Article 53(2) of Regulation (EU) 2019/881 if the investigation establishes a failure to comply with the requirements set out in Regulation (EU) 2019/881 or the European Cybersecurity Certification Scheme;

5) withdraw the validity of a European Cyber Security Certificate issued by itself or by a conformity assessment body in accordance with Article 56(6) of Regulation (EU) 2019/881, where an investigation establishes that the European Cyber Security Certificate does not comply with a requirement set out in Regulation (EU) 2019/881 or the European Cyber Security Certification Scheme;

6) restrict, suspend, revoke the additional ţgranting of the conformity assessment ţstaigq or lift the restriction or suspension of the additional ţgranting ţgranting ţ in the cases provided for in Article 35 of this Law.

6. The instructions and recommendations provided for in paragraph 5(2) of this Article shall be issued within 20 working days from the date of the decision.

7. Decisions of the National Cyber Security Centre, with the exception of the decision referred to in paragraph 5(3) of this Article, may be appealed against before a court in accordance with the procedure laid down in the Law on Administrative Proceedings.

VII CHAPTER

FRAMEWORK FOR THE USE OF THE SECURE NATIONAL DATA NETWORK

37 Article. Secure national data network

1. State and municipal institutions and bodies, state-owned enterprises and public bodies (hereinafter together referred to as 'institutions') registered on the list of users of the Secure State Data Network (hereinafter referred to as 'the Secure Network'), shall only use the electronic communication services provided by the Secure Network and shall only connect to the public electronic communication network through the Secure Network, except where the use of electronic communication services and/or connection to the public electronic communication network other than through the Secure Network is necessary for the purpose of gathering and/or providing intelligence. Where it is not technically possible to connect to the public electronic communications network only through the Secure Network, the authorities shall have the right to connect to the public electronic communications network outside the Secure Network in the cases and in the procedure established by the Government or its authorised body. The list of users of the Secure Network shall be approved by the Government on the proposal of the Minister of National Defence. Entities not included in the list of users of the Secure Network may not use the Secure Network. The Minister of National Defence shall review the list of users of the Safety Net at least once a year and, if necessary, initiate amendments to this list.

2. {Institutions meeting at least one of the following criteria shall be added to the list of users of the secure network:

1) the institution owns or manages State information resources necessary for the performance of vital State functions and State mobilisation tasks;

2) the institution, in the performance of vital State functions, is involved in the performance of State mobilisation tasks which require the transfer of data to, and/or the receipt of data from, institutions which manage and/or maintain State information resources necessary for the performance of vital State functions and State mobilisation tasks;

3) the institution is identified in the opinion of an authority authorised by the Government as being necessary for national security, defence or the exercise of vital State functions;

4) the institution, in the performance of its functions, needs to use the Secure Network or requires access to an institution or data centre located in the Member States of the European Union, the countries of the European Economic Area and/or NATO Member States.

3. The security network shall be managed by the Ministry of National Defence and administered by a state budget agency authorised by the Minister of National Defence.

4. The specific organisational and technical requirements applicable to the Safety Net, to the services of the Safety Net and to the providers of goods and services to the Safety Net, and to the Safety Net

Regulations shall be approved by the Manager of the Safety Net. The Safety Net Manager shall ensure the implementation of the specific organisational and technical requirements applicable to the Safety Net, as well as the provision of the Safety Net's standard and supplementary electronic communication and cybersecurity service. The conditions and rules for the provision of electronic communications and cyber security services provided through the Safety Net shall be laid down by the Government or by the body authorised by it. The goods and services necessary for the operation of the secure network shall be procured in accordance with the requirements of the Law on Public Procurement of the Republic of Lithuania.

5. The standard electronic communications and cyber security services (hereinafter referred to as "standard services") provided by the secure network shall include:

1) data rates set by the operator of the safety net transmission to users of the secure network and its structural units;

2) access to the public communications network at a speed set by your network manager;

3) collective protection through cyber-security measures;

4) interoperability with information resources managed by the European Union and its Member State authorities;

5) interconnection of parts of State-managed electronic communication networks used for State mobilisation tasks;

6) technical cooperation measures to ensure interoperability between the users of the Secure Network and their respective strulctiiriniq units.

6. The quantitative and qualitative indicators of the standard services shall be defined by the Government or its

The ¡authorised body shall provide electronic communications and cyber security services over the secure network in the terms and conditions and rules. The Safety Net Manager shall ensure the provision of standardised services free of charge to users of the Safety Net. The costs of the provision of the standardised services free of charge shall be paid from the State budget allocated for the management of the Safety Net and/or from any other means of financing provided for by law.

7. The additional electronic communications and cyber security services (hereinafter referred to as 'additional services') provided by the Safety Net shall consist of the services referred to in paragraph 5 of this Article, the quantitative or qualitative indicators of which, taking into account the needs of the users of the Safety Net, differ from the indicators of the established standard services.

8. The criteria for determining the amount of remuneration for the use of ancillary services shall be established and the description of the procedure for calculating the remuneration shall be approved by the Government. The Minister of National Defence, taking into account the criteria for the remuneration for the use of the Secure Network, shall determine the remuneration for the use of the Secure Network. The remuneration for additional services shall not exceed the cost of providing such services. The costs of the provision of additional services in the forests of the Security Grid Manager shall be verified by an auditor or auditing company and the verified data on the costs incurred shall be submitted to the Government within 2 months from the end of the calendar year

authority. The Government's delegated authority shall assess whether the remuneration for the provision of the ancillary service has been set in accordance with the criteria for setting the remuneration for the use of the ancillary service as laid down by the Government, and shall report to the Safety Net Manager with its conclusion.

9. The conditions, plan and time limits for the connection and disconnection of an institution to the safety net shall be determined by the Government or its granted authority.

38 Article 2. Use of the Data Centre

1. Institutions listed in } List of users of the secure network, except intelligence authorities, shall store the State information resources under their control in State data centres or in data centres located in the Republic of Lithuania or in other Member States of the European Union, the European Economic Area and/or NATO Member States, in accordance with the provisions of Article 45, Paragraphs 1 to 4, and Paragraphs 6 of the Law on the Management of State Information Resources. {Intelligence authorities on the list of users of the secure network shall store the State information resources under their control in data centres under their control, and copies of the data constituting the State information resources and of the information system in which these data are processed may, by decision of the head of the intelligence authority, be stored in data centres in the Republic of Lithuania or in data centres in the Republic of Lithuania or in the other Member States of the European Union, in the States of the European Economic Area, and/or in the Member States of NATO.

2. Total expenditure incurred by the institution in de1... on public information resources and/or public information resources under its control

storage of copies of such information in State data centres or in data centres located in the Republic of Lithuania or in other Member States of the European Union, the European Economic Area and/or NATO Member States, shall be paid from the State budget allocated to these institutions and/or from any other source of funding provided for in the legal acts regulating the activities of these institutions.

3. The list of State data centres, the technical and organisational requirements applicable to State data centres and to data centres located in the Republic of Lithuania or in other Member States of the European Union, in the countries of the European Economic Area and/or in NATO Member States, where State information resources are stored, shall be established in accordance with the procedure laid down in the Law on the Management of the State Information Resources.

Annex 1 to the Law on Cyber Security of the Republic of Lithuania

SECTORS OF CRITICAL IMPORTANCE

Sector	Sub-sector	Entity rfiche	Authority responsible for Identification
1. Energy	1.1. Electricity	1.1.1. Electricity companies, having the function of supplying electricity.	Lithuania Ministry of Energy of the Republic of Lithuania
		1.1.2. Electricity distribution companies grid operator.	Energy Ministry of Energy
		1.1.3. Electricity transmission system operator.	Energy Ministry
		1.1.4. Electricity producer.	Ministry of Energy
		1.1.5. Designated electricity Designated electricity market operators, as defined in Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on1 electricity internal market, Article 2(8).	Energy Ministry of Energy
		1.1.6. Electricity Energy Markets Participants as defined in Article 2(25) of Regulation (EU) 2019/943 providing electricity demand aggregation, energy storage services and electricity energy regulation load regulation services.	Energy Ministry of Energy
		1.1.7. Elektromobiliq |charging access operators.	Energy Ministry
	1.2 Centralised heat and water supply	1.2.1. Centralised heat or heat energy supply operators.	Energy Ministry
	1.3. Oil	1.3.1. Company operating oil pipelines.	Energy Ministry of Energy
		1.3.2. Oil refining ţmonê. Petroleum importing |monê, oil }importing ţ company, oil stockpiler ţ company, oil reserves a company that manages oil reserves.	Ministry of Energy
		1.3.3. Central storage and management company for petroleum products and oil stocks organisation.	Ministry of Energy
	1.4. Gas	1.4.1. Natural gas supply company.	Energy Ministry

Sector	Subsector	Boundary of the entity	Authority responsible for identification
		1.4.2. Gamtiniq gasq distribution system operator.	Energy Ministry
		1.4.3. Gamtiniq dujq transmission system operator.	Energy Ministry
		1.4.4. Gamtiniq dujq storage system operator.	Energy Ministry
		1.4.5. Liquefaction natural gas dujq system operator.	Energy Ministry
		1.4.6. Natural Gas Company.	Energy Ministry
		1.4.7. natural gas processing and processing plant operators.	Energy Ministry
	1.5. Hydrogen	1.5.1. Hydrogen production, storage and Transmission operators.	Energy Ministry
2. Transport	2.1. Air Transport	2.1.1. Air carriers as defined in 2008 as defined by the European Parliament and the Council on 11 March 2008 Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 April 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, are used for commercial purposes.	Ministry of Transport and Communications of the Republic of Lithuania
		Airport, including 2013 11 December 2013 of the European Parliament and of the Council Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on guidelines for the development of the trans-European transport network of the Union and repealing Decision No 661/2010/EU, the main airports listed in Section 2 of Annex II, and the head of the ţmonês managing the airport. Entities operating ancillary facilities at airports.	Contact Ministry of Transport
		2.1.3. air traffic management operators providing air traffic management services as defined in Article 2.1.2 of the Treaty of the European Parliament and of the Council of 10 March 2004 Regulation (EC) No 549/2004 of the Council of 10 March 2004 laying down the framework for the creation of the single European sky.	Ministry of Transport and Communications
	2.2. Railways Transport	2.2.1. Railways infrastructures Manager.	Transport Ministry
		2.2.2. Railway company (carrier).	Ministry of Transport and Communications

Sector	Sub-sector	Entity heading	Authority responsible for Identification
		2.2.3. Railway service ţ installations Operator.	Transport Ministry of Transport
	2.3 Water transport	2.3.1. Inland waterway, jürq and coastal passenger and freight water transport companies, as defined in relation to jfiru transport on 31 March 2004. Regulation (EC) No 725/2004 of the European Parliament and of the Council on ship and port security security enhancement in Annex I, not including tq companies operated by an individual ship.	Ministry of Transport and Communications
		2.3.2. Companies and entities operating ports, including port facilities as defined in Article 2(11)of Regulation (EC) No 725/2004, which carry out port-based |the operation, management and maintenance of port facilities.	Ministry of Transport and Communications
		2.3.3. Laivq traffic tamybq operators.	Contact Ministry
	2.4. Transport	2.4.1. Ke1iq directorates, as apibrêžta 18 December 2014. Article 2(12) of Commission Delegated Regulation (EU) No 2015/962 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to real-time traffic information services throughout the European Union, responsible for the control of traffic management, except for the public entities for which the activities of a traffic management or intelligent transport system operator are exclusively a minor part of their overall activities.	Transport Ministry of Transport
		2.4.2. Intelligent Transport System operators.	Ministry of Transport Ministry
3. Banking		3.1.1 Credit institutions as defined in Article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012.	Ministry of Finance of the Republic of Lithuania

Sector	Sub-sector	Entity Boundary	Authority responsible for Identification
4. Financial market infrastructures		4.1.1. Trading venue operators.	Ministry of Finance
		4.1.2. central counterparties as defined in Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council of 26 June 2013 on OTC derivatives, central counterparty and transaction data repositoryq 2 point 1.	Finansq Ministry
5. Health care		5.1.1. Personal health care health care institution.	Lithuanian Republic of Lithuania Ministry of Health of the Republic of Lithuania
		5.1.2. the European Union reference laboratories referred to in Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on the serious cross-border threats health, which repealing Decision No 1082/2013/EU, Article 15.	Ministry of Health
		5.1.3. Entities, operating a medicinal product (pharmaciniq preparation), scientific research and development activities.	Health Ministry of Health
		5.1.4. Entities producing basic pharmaceutical products and pharmaceutical preparations listed in the Economic activities of the Classification of Economic Activities 2 Section C, Chapter 21.	Ministry of Health
		5.1.5. Entities producing medical devices considered to be of critical importance in the event of a public health emergency (list of critical medical devices in the event of a public health emergency), within the meaning of Regulation (EU) 2022/123 of the European Parliament and of the Council of 25 January 2022 on the reinforced role of the European Medicines Agency in the preparation of the European Medicines Agency for medicinal products and medical	Ministry of Health

Sector	Subsector	Subject heading	Authority responsible for identification
		measure in the area of crisis and its management Article 22	
6. Drink Water		6.1.1. Water for human consumption suppliers and distributors, except distributors for whom the distribution of water for human consumption is an insignificant part of the distribution of jq general other goods and productsq activities.	Lithuania Ministry of the Environment of the Republic of Lithuania
7. Sewage		7.1.1. undertakings collecting, disposing of or treating waste water, except undertakings for which the collection of urban waste water, domestic waste water or industrial waste water , disposal or treatment is a non-essential part of their general activities.	Environment Ministry
8. Digital infrastructure		8.1.1. Internet dataq flow to the providers of the small point.	Communications Ministry
		8.1.2. Domain nameq systems service providers.	Lithuania Republic of Lithuania Economy and Innovationq Ministry of Innovation and Innovation
		8.1.3. Supreme level Domainq vardq registration providers.	Economic and Ministry of Innovation
		8.1.4. Cloud service providers.	Economic and Innovation Ministry
		8.1.5. Dataq centreq servicesq providers.	Economic and Ministry of Economy and Innovation
		8.1.6. Distributed content provision network providers.	Economic and Innovationq Ministry
		8.1.7. Reliability assurance service providers.	Economic and Ministry of Innovation
		8.1.8. Public Qjq electronic public electronic communication network providers.	Contact Ministry of Communications
		8.1.9. Public electronic public electronic communication service providers.	Communications Ministry of Communications
9. Management of information and communication technology services (services		9.1.1. Managed service providers.	Ministries
		9.1.2. Managed cybersecurity service providers.	Ministries

Sector	Subsector	Entity rüiis	Institution, responsible for identification
"business business to business")			
10. Public Administration		10.1.1. Administration Entities.	Lithuanian Ministry of the Interior
		10.1.2. Regional Administration Entities and regional and municipal administration entities.	Internal affairs Ministry
11. Kosmos		11.1.1. space objects established by the Republic of Lithuania or owned, managed and operated by private entities operators of terrestrial infrastructure which support the provision of space services, with the exception of providers of public electronic communications networks.	Ministry of Economy and Innovation

Annex 2 to the Law on Cyber Security of the Republic of Lithuania

OTHER SECTORS OF CRITICAL IMPORTANCE

Sector	Sub-sector	Entity rfiche	Authority **responsible for the entity** Identification
1. Postal services		1.1.1. Postal service providers.	Lithuanian Ministry of Transport and Communications of the Republic of Lithuania
2. Performed by management		2.1.1. Waste management service providers, except service providers whose main economic activity is not waste management.	Lithuania Republic of the Environment Ministry
3. Cheminiq production and distribution of materials		3.1.1. Chemines materials undertakings manufacturing and distributing chemical substances or mixtures as defined in Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 on the registration of chemicals substances , registration, evaluation, authorisation and restriction	Environment Ministry of Environment

Sector	Subsector	Entity rfisis	Authority responsible for the entity Identification
		(REACH), |steigiančio Europos cheminiq medžiagq agentūrą, iš dalies keičiančio Direktyvą 1999/45/EB bei panaikinančio Tarybos reglamentą (EEB) Nr. 793/93, Komisijos reglamentą (EB) Nr. 1488/94, Tarybos direktyvą 76/769/EEB ir Komisijos direktyvas 91/155/EEB, 93/67/EEB, 93/105/EB bei 2000/21/EB, 3 straipsnio 9 ir 14 punktuose, ir gaminius, kaip apibrê“zta to paties reglamento 3 straipsnio 3 punkte, iš tą medžiagq ar mixture from the undertaking producing the substance or mixture.	
4. Food production, processing and distribution		4.1.1. food businesses, as defined in Article 3(2) of Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety, carrying out wholesale distribution and industrial production and processing activities.	Lithuanian Ministry of Agriculture of the Republic of Lithuania
5. Production	5.1. Manufacture of medical devices and *in vitro* diagnostic medical devices	5.1.1 Entities manufacturing medical devices as defined in Article 2(1) of Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC and *in vitro* diagnostic medical devices as defined in Article 2(2) of Regulation (EC) No 178/2002 and repealing Council Directives 90/385/EEC and 93/42/EEC entities manufacturing in vitro diagnostic medical devices, as defined in Article 2(2) of Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices, repealing Directive 98/79/EC and Commission Decision 2010/227/EU, with the exception of entities listed in Annex I to this Regulation referred to in point 5.1.5 of medical devices.	Ministry of Health of the Republic of Lithuania

Sector	Subsector	Entity heading	Authority responsible for the entity Identification
	5.2. Computer, electronic and optical products manufacturing	5.2.1. Entities engaged in any of the economic activities listed in the Economic activity Section C of the Classification of Economic Activities, Revision 2 of the NACE Rev. 2 Chapter 26.	Economic and Innovation Republic of Lithuania Ministry of Industry and Innovation
	5.3. Electricity Electricity generation	5.3.1. Entities carrying out any of the economic activities listed in activity Section C of the Classification of Economic Activities, Revision 2 of the NACE Rev. 2 Chapter 27.	Ministry of Energy of the Republic of Lithuania
	5.4. Manufacture of machinery and equipment n.e.c.	5.4.1. Entities engaged in any of the following economic activity listed in the Economic activity in Section C, Chapter 28 of Revision 2 of the Classification.	Ministries
	5.5 Motor vehicles, trailers and semi-trailers manufacturing	5.5.1. Entities engaged in any of the economic activities listed in the Economic activity Chapter 29, Section C, Revision 2, Chapter 29 of the Classification of Economic Activities.	Ministry of Transport
	5.6 Manufacture of other transport equipment	5.6.1. Entities carrying out any of the economic activities listed in the Economic activity Chapter 29, Section C, Chapter 29 of the Classification of Economic Activities, Revision 2 of the Classification.	Ministry of Transport and Communications
6. Information public services		6.1.1. Electronic marketplaceq service providers.	Economic and Ministry of Innovation
		6.1.2. Search engine providers.	The Ministry of Economy and Innovation Ministry
		6.1.3. Socialiniq network service for platform providers.	Economic and Ministry of Innovation
		6.1.4. Electronically information hosting service for providers.	The Ministry of Economy and Innovation Ministry
7. Scientific Research		7.1.1. Entities carrying out research.	Ministry of Education, Science and Sport of the Republic of Lithuania

Annex 3 to the Law of the Republic of Lithuania on Cyber Security

IMPLEMENTATION OF EUROPEAN UNION LEGISLATION

1. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the cybersecurity certification of ENISA (European Union Agency for Cyber Security) and of information and communication technologies and repealing Regulation (EU) No 526/2013 (the "Cyber Security Act").

2. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing a European Centre of Excellence for Cyber Security Industry, Technology and Research and a network of National Coordination Centres.

3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity throughout the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (IIA 2 Directive).

Article 2. Entry into force, implementation and application

1. This Law, with the exception of paragraph 2 of this Article, shall enter into force on 18 October 2024.

2. The Government of the Republic of Lithuania, the Minister of National Defence and the Director of the National Cyber Security Centre shall adopt the legal acts implementing this Law before 17 October 2024.

3. The National Cyber Security Centre shall identify the following by 17 April 2025

cybersecurity entities operating in the sectors referred to in Annexes 1 and 2 to the Law on Cybersecurity of the Republic of Lithuania set out in Article 1 of this } Law, which comply with the provisions of this

cybersecurity entities which comply with the requirements laid down in Article 11 of the Law on Cybersecurity laid down in Article 1 of this } Law and shall include them in the Cybersecurity Information System.

4. Entities which, prior to the date of entry into force of this Law, were included in the } the list of critical information infrastructure and its managers approved by the Government until 17 April 2025, shall continue to ensure that the network and information system under their management comply with the requirements set out in the list of critical information infrastructure and its managers before this

The organisational and technical cybersecurity requirements for cybersecurity entities set out in Article 11(1)(1)(1) of the Law of the Republic of Lithuania on Cybersecurity in force at the effective date of the entry into force of the Law.

5. Entities which, before the date of entry into force of this Law, were included in the list of critical information infrastructure and its managers approved by the Government, and which were included in the Register of Cyber Security Entities, shall be obliged to continue to ensure that the network and information system under their management comply with the cyber security requirements laid down in Article 11(1)(1) of the Law on Cyber Security, which were in force before the date of entry into force of this Law, applicable to cybersecurity entities, as long as the obligation to ensure compliance of the network and information system under its control with the cybersecurity risk management measures referred to in Article 14(1) of the Cybersecurity Law, as laid down in Article 1 of this Law, arises.

6. Security Agents who, prior to the entry into force of this Law, were subject to the provisions of Article 22 of the Law on Cybersecurity regarding the appointment and eligibility of the Security Agent shall continue to perform their duties in accordance with the procedure laid down in Article 15 of the Law on Cybersecurity issued under Article 1 of this Law. The requirements referred to in Article 15(5)(3) of the Cybersecurity Law as laid down in Article 1 of this Law shall not apply to the security jgeneral referred to in this paragraph for a period of the first 2 years following the date of entry into force of this Law.

7. The National Cyber Security Centre shall, in the cases referred to in paragraphs 4 and 5 of this Article, supervise the compliance of the communication and information system with the organisational and technical cyber security requirements for cyber security entities and shall have the powers referred to in Article 8(2)(2), (4), and (5) of the Law on Cyber Security in force prior to the d a t e of entry into force of this ţlaw.

8. In the cases referred to in paragraphs 4 and 5 of this Article, the National Cyber Security Centre shall apply the provisions of Article 480(4) and (5) of the Administrative Code of the Republic of Lithuania in force before the date of entry into force of this Law, if it detects a violation of the organisational and technical cyber security requirements for cyber security entities, as set out in Article 11(1)(1) of the Law on Cyber Security, which was in force before the date of entry into force of this Law.

9. Procedures initiated in accordance with the Law on Cybersecurity in force prior to the date of entry into force of this Law shall be continued and concluded in accordance with the provisions of the Law on Cybersecurity in force prior to the date of entry into force of this Law and the legal acts implementing it.

10. The term 'communication and information system' used in other legal acts shall correspond to the term 'network and information system' used in the Cybersecurity Law laid down in Article 1 of this Law.

11. The Government shall prepare and submit to the Seimas of the Republic of Lithuania, by 1 June 2025, a draft law regulating the legal regulation of the operation of state-owned non-public electronic communications networks.

Article 3. *Ex-post* evaluation of the existing legal regulation laid down in the Law

1. The Ministry of National Defence of the Republic of Lithuania shall carry out an *ex-post* evaluation of the impact of the existing legal regulation on cybersecurity set out in the Law on Cyber Security set out in Article 1 of this Law (hereinafter referred to as the *ex-post* evaluation).

2. The *en-post* evaluation shall determine the impact on cybersecurity actors of the measures laid down in the Cybersecurity Law, as set out in Article 1 of this Law, relating to cybersecurity.

3. *The ex post* evaluation period is 3 years from the date of entry into force of this Law.

4. *The ex-post* evaluation must be carried out by 1 January 2029.

I hereby promulgate this law adopted by the Seimas of the Republic of Lithuania.

The President of the Republic  Gitanas Nausėda