Translated by the Ministry of National Defence

REPUBLIC OF LITHUANIA LAW
ON CYBER SECURITY

11 December 2014 No. XII-1428

Vilnius

(As last amended on 27 June 2018 – No XIII-1299)

CHAPTER I
GENERAL PROVISIONS

Article 1. Purpose and Application of the Law

1. This Law establishes cyber security principles, specifies institutions which develop and implement cyber security policy, defines powers of such authorities in the field of cyber securities, and determines duties of cyber security entities as well as inter-institutional cooperation.

2. This Law shall not apply to trust service providers which are subject to the requirements laid down in Article 19 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, (OJ 2014 L 257, p. 73).

3. The provisions of this Law are harmonised with the legal acts of the European Union specified in the Annex to this Law.

Article 2. Definitions

1. **Cloud computing services** shall mean services the recipients of which use the infrastructure of communications and information systems controlled by these service providers at a distance.

2. **Digital information hosting services** shall mean services which comprise the provision of opportunities to use tools for the development and management of electronic

information and digital data (hereinafter referred to as the "digital information") and/or storage of digital information supplied by the service provider.

3. **Electronic marketplace service(s)** shall mean service(s) which provide consumers and/or commercial entities with opportunities to conclude agreements on electronic trade or service agreements with commercial entities on an e-marketplace website or on the website of a commercial entity on which computing services provided on the online market are used.

4. **Critical information infrastructure** shall mean a communications and information system or part of it, a group of communications and information systems the occurrence of a cyber incident in which might have a major negative impact on the national security, economy of the country, and interests of the state and the public.

5. **Manager of the critical information infrastructure** shall mean a person who manages the critical information infrastructure.

6. **Cyberspace** shall mean the environment which is composed of computers and other communications and information technology equipment and digital information generated in such computers and equipment and/or transmitted using them.

7. **Cyber security crisis** shall mean a cyber incident or incidents the negative effect of which cannot be eliminated by the Republic of Lithuania on its own or which have a negative impact on the Republic of Lithuania and other states which are members of international organisations and to which the Republic of Lithuania belongs or on the authorities of such international organisations of such extent in terms of technical and political aspects that a need to coordinate politics and respond to them on an international level occurs.

8. **Cyber security entity** shall mean an entity which controls and/or manages information resources of the state, manager of critical information infrastructure, service provider of public communications networks and/or public digital communication services, provider of digital information hosting services and providers of digital services.

9. **Cyber incident** shall mean an event or activity in cyber space which might pose or poses threat or has a negative effect on the accessibility, authenticity, integrity and confidentiality of digital information transmitted by use of communications and information systems or processed in such systems, also which might disrupt or disrupt the operation, management of communications and information systems and the provision of services to such systems.

10. **Cyber security** shall mean the totality of legal, information distribution, organisational and technical measures which are aimed at maintaining resistance to factors which pose threat to communications and information systems in cyber space or to the accessibility, authenticity, integrity and confidentiality of digital information transmitted by or processed in

such systems, to non-disruptive operation, management of communications and information system or provision of services to these systems, also which serve to restore the usual operation of the communications and information systems.

11. **Cyber incident management** shall mean the procedures which aim at detecting, analysing cyber incidents and responding to them as well as at restoring the usual operation of the communications and information systems.

12. **Online search services** shall mean services whereby the internet users are given the opportunity to perform search on websites according to a query on a certain subject matter using a keyword, a phrase or any other input data. The search delivers links which might contain information related to the content searched for.

13. **Industrial process management system** shall mean a system composed of equipment based on communications and information technology which is intended for monitoring technological processes or managing industrial, energy, transport, water supply services and services in other areas of economic activity.

14. **Communications and information system** shall mean a network of electronic communications, an information system, a registry, industrial process management system and digital information retained, processed, restored or transmitted for the purpose of their management, use, protection and maintenance.

15. **Risk** shall mean a reasonably identified fact or event which might negatively affect the security of communications and information system.

16. **Digital services** shall mean a group of services based on communications and information technology which encompasses the services of e-market, web search and/or cloud computing.

17. **Digital service provider** shall mean a legal entity which provides digital services in the Republic of Lithuania and/or other EU Member States.

18. The criteria on the basis of which the assessment is made of whether the negative impact specified in Article 2(4) is major shall be determined in the methodology for identification of critical information infrastructure.

19. Other terms used in this law shall be understood the way they are defined in the Republic of Lithuania Law on Electronic Communications, the Republic of Lithuania Law on Management of State Information Resources, the Republic of Lithuania Law on Information Society Services, the Republic of Lithuania Law on Legal Protection of Personal Data, the Republic of Lithuania Law on Intelligence, the Republic of Lithuania Law on Criminal Intelligence, the Republic of Lithuania Law on Prohibition of Unfair Practices of Retailers, the Republic of Lithuania Law on Small and Medium-Sized Business Development and Regulation

(EU) No. 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 of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (OJ 2012 L 316, p. 12).

Article 3. Cyber Security Principles

1. Cyber security is based on the following key cyber security principles:

1) non-discrimination of cyber space, which means that the provisions of legislation are applied and benefits are stored both in physical and cyber space equally;

2) management of cyber security risk, which means that the applicable cybersecurity measures must ensure that regularly assessed risks of cyber security entities are captured;

3) proportionality of cyber security, which means that legal, organisational and technical cyber security measures, which are applied, shall not restrict the activities of cyber security entities in cyber space more than required;

4) supremacy of public interest, which means that the applicable cyber security measures shall first guarantee the protection of public interest, however, shall not, in principle, infringe on consumer rights or limit their freedom in cyber space proportionally;

5) standardisation and technological neutrality, which means that when implementing cyber security measures, cyber security entities shall be encouraged to follow the national, the EU and other international communications and information systems' cyber security standards and specification, without demanding to apply any specific type of technology and without giving it the priority;

6) subsidiarity, which means that cyber security entities, which operate information systems and use them for the provision of services, are responsible for cyber security of information systems as well as for services which are provided using such systems. In the areas which fall within the exclusive competence of cyber security entities, the authorities which develop and implement cyber security policy shall take measures solely when cyber security of the communications and information systems and services provided using such systems cannot be ensured by cyber security entities which manage such systems and use them for the provision of services.

2. When applying legal provisions which regulate cyber security, consideration shall be taken of the principles set forth in Article 3(1). These principles shall be inter-aligned and coordinated; neither of them shall be given priority or prevalence.

CHAPTER II
DEVELOPMENT AND IMPLEMENTATION OF CYBER SECURITY POLICY

Article 4. Authorities Developing and Implementing Cyber Security Policy

1. Strategic goals and priorities of cyber security policy as well as measures necessary to achieve them are determined by the Government of the Republic of Lithuania.

2. Cyber security policy is developed, its implementation is organised, controlled and coordinated by the Ministry of National Defence of the Republic of Lithuania. The National Cyber Security Centre takes part in the development of the cyber security policy to the extent to which legal regulation of activities of cyber security entities has to be established for the performance of functions laid down in this law.

3. Cyber security policy is implemented by the National Cyber Security Centre, the State Data Protection Inspectorate, the Lithuanian Police and other authorities the functions of which are related to cyber security.

Article 5. Powers of the Government in the field of cyber security

The Government:

1) approves the National Cyber Security Strategy;

2) approves the institutional composition of the Cyber Security Council;

3) approves the methodology for identification of critical information infrastructure and the list of critical information infrastructure and its managers;

4) approves organisational and technical cyber security requirements imposed on cyber security entities;

5) approves the National Cyber Security Management Plan;

6) supervises cyber security crisis management.

Article 6. Powers of the Ministry of National Defence in the field of cyber security

The Ministry of National Defence:

1) coordinates the preparation of the National Cyber Security Strategy, submits it to the Government for approval;

2) submits to the Government organisational and technical cyber security requirements imposed on cyber security entities for approval;

3) submits the National Cyber Incident Management Plan to the Government for approval;

4) submits the methodology for identification of critical information infrastructure to the Government for approval;

5) submits the list of critical information infrastructure and its managers to the Government for approval;

6) approves a typical plan for cyber incident management in critical information infrastructures;

7) approves a cyber defence plan for critical information infrastructures;

8) establishes the procedure for responding to cyber incidents, which occur in communications and information systems of cyber security entities, by the National Cyber Security Centre;

9) approves the plan on implementation of technical cyber security measures, establishes the procedure for their implementation and management in information resources and in critical information infrastructure;

10) participates in cyber security crisis management;

11) establishes Cyber Security Information Network and approves its regulations;

12) approves the Regulation of the Cyber Security Council and composition.

Article 7. Cyber Security Council

1. The Cyber Security Council is a permanent collegial independent advisory body which analyses the situation of cyber security assurance in the Republic of Lithuania and puts forward proposals to institutions which develop and implement cyber security policy, cyber security entities, research and educational institutions and business entities which engage in activities in the field of information technology (hereinafter referred to as the "Cyber Security Actors") with regard to improvement of the situation of cyber security assurance.

2. The Cyber Security Council is headed by a representative of the Ministry of National Defence.

3. The provision of commodities and technical maintenance of the Cyber Security Council is taken care of and ensured by the Ministry of National Defence or its authorised institution.

4. The Cyber Security Council:

1) submits suggestions to the Cyber Security Actors with regard to cyber security priorities, development directions, target results and ways the objectives are to be pursued;

2) submits suggestions to the Cyber Security Actors with regard to opportunities of cooperation between the public sector, business and research in the field of cyber security assurance;

3) analyses the trends of improvement of cyber security assurance, delivers conclusions and proposals with regard to cyber incident management to Cyber Security Actors;

4) provides recommendations to the Cyber Security Actors with regard to enhancement of cyber security.

Article 8. National Cyber Security Centre

1. The National Cyber Security Centre is an institution, which is subordinate to the Ministry of National Defence.

2. When implementing the cyber security policy, the National Cyber Security Centre:

1) conducts the supervision of compliance of the cyber security entities and communications and information systems managed by them with organisational and technical cyber security requirements imposed on cyber security entities as well as carries out survey on the cyber security situation;

2) gives orders to cyber security entities to provide information necessary for the compliance of the cyber security entities and communications and information systems managed by them with organisational and technical cyber security requirements imposed on cyber security entities, and to conduct the assessment of the cyber security situation;

3) applies technical measures so as to measure the resistance of the state's information resources and critical information infrastructures to cyber incidents;

4) gives orders in relation to assurance of cyber security and removal of identified cyber security defects, sets the deadline for the fulfilment of orders by the entities which control and/or manage the state's information resources, by managers of critical information infrastructure, providers of public communications networks and/or public electronic relations services and digital information hosting service providers;

5) gives directions to cyber security entities, excluding digital service providers, to conduct an independent communications and information systems or services provided using such systems at their own expense and deliver the results of such audit, if they fail to provide technical information necessary for the assessment of the cyber security situation with regard to communications and information systems or services provided using such systems as set forth in the description of organisation and technical cyber security requirements imposed on cyber security entities;

6) upon receipt of evidence from a cyber security entity, a user of digital service or any other EU Member State in which digital services are provided, from a competent authority which supervises the activities of digital service providers in the field of cyber security which states that digital service providers fail to meet the requirements laid down in this law, gives directions

to digital service providers to provide information necessary for the assessment of cyber security of communications and information systems managed by them and to remove the defects of implementation of cyber security requirements;

7) monitors cyber incidents on the national level and carries out cyber incident analysis;

8) in accordance with the plan on implementation of cyber security measures coordinated with the entities which control and/or manage the state resources or with the managers of critical information infrastructure in compliance with the procedures established of the Minister of National Defence, implements and controls technical cyber security measures in the state's information resources and critical information infrastructure. Measures implemented using the funds of the National Cyber Security Centre shall be used exclusively for the assurance of cyber security. Technical measures implemented using the funds of the National Cyber Security Centre shall be maintained and their repair shall be conducted by the funds of the National Cyber Security Centre;

9) organises management of cyber incidents in communications and information systems of cyber security entities on a national level;

10) puts cyber security measures into use in the event of a cyber incident;

11) to stop the spread of effects of cyber incidents on cyber security of the state's information resources or critical information infrastructure, orders the providers of public communications networks and/or public electronic communications service providers to limit the provision of public communications networks and/or public electronic communications services for no longer than 48 hours to the recipient of the services. The National Cyber Security Centre shall notify the Communications Regulatory Authority of the Republic of Lithuania of the orders given to the providers of public communications networks and/or public electronic communications service providers under this clause no later than the next business day;

12) participates in the management of cyber security crises;

13) where necessary to inform the public so as to avoid a cyber incident or to capture the on-going cyber incident, having consulted the cyber security entity, informs the public about individual cyber incidents and requests the cyber security entity do the same;

14) cooperates with competent authorities of international organisations, with cooperation groups established by them as well as with foreign competent authorities and services; has the right to address them so as to fulfil the functions provided for in this law and other legislation in the field of cyber security in cooperation;

15) processes personal data, necessary for the fulfilment of the functions of the National Cyber Security Centre in the field of cyber security assurance. The National Cyber Security

Centre processes personal data in accordance with the procedure established in the Law on Legal Protection of Personal Data;

16) in cooperation with business entities, research and education institutions and cyber security entities, develops projects which strengthen the national cyber security;

17) fulfils the functions set forth in legal acts of the Republic of Lithuania in the field of cyber security assurance.

Article 9. Powers of the State Data Protection Inspectorate in the field of cyber security

The State Data Protection Inspectorate implements the cyber security policy in the field of protection of personal data and fulfils the tasks established by the supervisory authority in accordance with 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 (General Data Protection Regulation) (OJ 2016 L 119, p. 1).

Article 10. Powers of the Police in the field of cyber security

When implementing the prevention of cyber incidents which possibly have constituent elements of criminal offences and when conducting their investigation, the Police:

1) collects, analyses and summarises information about cyber incidents which possibly have constituent elements of criminal offences;

2) establishes the procedure for the provision of information by cyber security entities to the police which is required to prevent and investigate cyber incidents which might have constituent elements of criminal offences;

3) where the service provider allegedly participates in or the communications and information technology equipment it uses is allegedly used for criminal offences, has the right without a court sanction to order the provider of public communications networks and/or public digital communications service providers, digital information hosting service providers and digital service providers to limit the provision of public communications networks and/or public electronic communications services, digital information hosting services and digital services to the recipient of services for no longer than 48 hours, and for a longer period – where the sanction of the district court is available and/or to order the service provider to apply measures which help remove the reasons for criminal offences in cyber space. In such cases the chairman of the district court or a judge authorised by him is provided with an offering with regard to the confirmation of lawfulness or reasonableness of actions on the basis of a reasoned ruling. Should

the deadline for the limitation of service provision specified in this clause expire at weekends or on public holidays, the proposal (offering) shall be submitted no later than the next business day or the next day after a public holiday. If a judge delivers a reasoned verdict whereby the legitimacy or reasonableness of the actions specified in the proposal is not approved, the order shall be immediately suspended;

4) has the right to issue an order to the provider of public communications networks and or public digital communications service provider, digital information hosting service provider and digital service provider to preserve information related to the services provided by them which might help detect the type of communications service used, technical measures which were applied and the times of usage, identify the recipient of services, mail address, geographical location address, phone or any other access number, information about accounts and payments made on the basis of service agreement and other information which is available in the location where communications equipment is installed, on the basis of the existing service contract or agreement, get this information, and with the court ruling substantiated available, to receive the data of service recipients' flow and control the content of transferred information specified herein.

CHAPTER III

OBLIGATIONS OF CYBER SECURITY ENTITIES

Article 11. General duties of cyber security entities

1. Cyber security entities:

1) are responsible for cyber security of communications and information service they manage and of services they provide, ensure their compliance with the organisational and technical cyber security requirements imposed on cyber security entities;

2) conduct risk assessment in accordance with the procedure established in the description of organisational and technical cyber security requirements imposed on cyber security entities as well as implement other technical and organisational cyber security measures based on the latest technology developments proportionate to the identified risk;

3) notify the National Cyber Security Centre of cyber incidents which occur in communications and information systems controlled and/or managed by them as well as of applied cyber indecent management measures in accordance with the terms and conditions as well as with the procedure laid down in the National Cyber Incidents Management Plan;

4) provide the Police with information required for the prevention and investigation of infringements of the law which have constituent elements of criminal offences in cyber space in accordance with the procedure established by the Police Commissioner General as well as

execute other orders of the police issued on the basis of this law. Police orders with regard to restriction of the provision of services to their recipients must be carried out no later than within 8 hours from the receipt of the police order;

5) assign a competent person or department responsible for the organisation and assurance of cyber security and provide the National Cyber Security Centre with the contact details of such person or department;

6) execute the orders of the National Cyber Security Centre set forth in Article 8 herein.

2. The provisions of this article shall not apply to small and very small undertakings as defined in the Law on Small and Medium-sized Business Development which provide digital services in the Republic of Lithuania and/or any other EU Member State.

Article 12. Special duties of cyber security entities

1. Managers of critical information infrastructure:

1) in accordance with the typical plan for cyber incident management in critical information infrastructures, approve plans on cyber incident management in critical information infrastructures and submit them to the National Cyber Security Centre;

2) notify digital service providers of negative impact on the operation of critical information infrastructure which resulted from malfunctioning of communications and information systems of digital service providers in accordance with the procedure established in the National Cyber Incident Management Plan;

3) no less than once a calendar year test the functioning of measures intended for the management of cyber incidents in critical information infrastructures and supply the results of testing to the National Cyber Security System in accordance with the procedure established in the description of organisational and technical cyber security requirements imposed on cyber security entities;

4) provide conditions for the National Cyber Security Centre to implement and control technical cyber security measures in critical information infrastructure and to put technical measures into use with the aim to measure the resistance of critical information infrastructure to cyber incidents.

2. Entities which control and/or manage the state's information resources provide conditions for the National Cyber Security Centre to implement and control technical cyber security measures in the state's information resources and to put technical measures into use with the aim to measure the resistance of the state's information resources to cyber incidents.

3. The providers of public communications networks and/or public digital communications services publicly announce recommendations with regard to measures meant to

assure cyber security by using services provided by public communications networks and/or public electronic communications services on their websites or by other means of mass media.

4. Digital information hosting service providers publicly announce on their websites or use any other means of mass media to publish recommendations to digital information hosting service providers with regard to measures meant to assure cyber security by use of digital information hosting services.

5. Digital service providers:

1) publicly announce on their websites or use any other means of mass media to publish recommendations to service providers with regard to measures intended to assure cyber security by use of services provided by digital service providers;

2) assign a representative to carry out activities on behalf of the digital service provider in the European Union. Such representative shall be a natural or a legal person established in one of those EU Member States in which digital services are provided. Cyber security policy implementation authorities have the right to address the representative of a digital service provider with regard to the performance of duties of a digital service provider set forth in this law. If a digital service provider assigns a representative to conduct activities in the Republic of Lithuania, it shall be deemed that the digital service provider is subject to the jurisdiction of the Republic of Lithuania.

6. The provisions of this article shall not apply to small and very small undertakings as defined in the Law on Small and Medium-sized Business Development which provide digital services in the Republic of Lithuania and/or any other EU Member State.

CHAPTER IV
EXCHANGE OF INFORMATION AND INTERINSTITUTIONAL COOPERATION

Article 13. Cyber Security Information Network

1. The purpose of the cyber security information network is to share information about potential or past cyber incidents, also recommendations, orders, technical solutions and other measures which help assure cyber security and cooperation among the members of the cyber security information network in the field of cyber security.

2. The cyber security information network can be used solely by those cyber security entities which meet the requirements set forth in the Regulations of the Cyber Security Information Network.

3. The cyber security information network serves to announce relevant contact information of persons or departments assigned by cyber security entities responsible for organisation of cyber security and management of cyber incidents.

Article 14. Inter-institutional cooperation in managing and investigating cyber incidents

1. The National Cyber Security Centre and the Police consult each other and cooperate in investigating cyber incidents, exchange information related to investigation of cyber incidents which is required to perform the functions of these authorities which fall under their competence. When required, investigation of cyber incidents might be reported to other entities of criminal intelligence and/or intelligence institutions.

2. The National Cyber Security Centre and the State Data Protection Inspectorate cooperate in investigating cyber incidents related to personal data and/or privacy protection violations, exchange information which is necessary for the fulfilment of functions established by legal acts in relation to investigation of cyber incidents which infringe on personal data and/or privacy protection.

3. The procedure of inter-institutional cooperation in managing and investigating cyber incidents shall be established in the National Cyber Incident Management Plan.

Article 15. Information Protection

The authorities implementing the Cyber Security Policy shall have the right to exchange the information provided by cyber security entities, including confidential information, to the extent to which this is necessary to fulfil the functions of such authorities under their competence and must ensure the protection of received information.

CHAPTER V
FINAL PROVISIONS

Article 16. Voluntary reporting about cyber incidents

1. Persons which under this law have no obligations to report about cyber incidents in the communications and information systems controlled by them shall have the right to notify the National Cyber Security Centre of cyber incidents and measures taken to capture cyber incidents on a voluntary basis. The National Cyber Security Centre processes such reports in accordance with the procedure established in the National Cyber Incident Management Plan.

2. A person that voluntarily reports about cyber incidents shall be imposed no obligations in relation to the submission of a report.

I promulgate this Law passed by the Seimas of the Republic of Lithuania

President of the Republic Dalia Grybauskaitė

Annex
to the Republic of Lithuania Law on
Cyber Security

IMPLEMENTED EUROPEAN UNION LEGISLATION

1. Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ 2004 *Special Edition*, Chapter 13, Volume 29, p. 349) with the latest amendments adopted by Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 37).

2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ 2016 L 194, p. 1).