THE CROATIAN PARLIAMENT

1305

Pursuant to Article 89 of the Constitution of the Republic of Croatia, I hereby issue the

DECISION

ON PROMULGATING THE ACT ON CYBERSECURITY OF OPERATORS OF ESSENTIAL SERVICES AND DIGITAL SERVICE PROVIDERS

I hereby promulgate the Act on Cybersecurity of Operators of Essential Services and Digital Service Providers, passed by the Croatian Parliament at its session on 6 July 2018.

Class: 011-01/18-01/79
Reg. No: 71-06-01/1-18-2
Zagreb, 10 July 2018

The President
of the Republic of Croatia
Kolinda Grabar-Kitarović, m. p.

ACT

ON CYBERSECURITY OF OPERATORS OF ESSENTIAL SERVICES AND DIGITAL SERVICE PROVIDERS

PART I

BASIC PROVISIONS

Subject and Scope

Article 1

(1) This Act establishes the procedures and measures for achieving a high common level of cybersecurity of operators of essential services and digital service providers, competences and powers of competent sectoral authorities, the single national point of contact, computer security incident response teams (hereinafter referred to as: competent CSIRT) and technical compliance evaluation authority, oversight of operators of essential services and digital service providers in the implementation of this Act and penalties.

(2) The objective of this Act is to ensure the implementation of measures for achieving a high common level of cybersecurity in providing services which are of special importance for key social and economic activities, including the functioning of the digital market.

(3) The following Appendices shall form an integral part of this Act:

a) Appendix I – List of essential services with criteria and thresholds for determining the significance of the incident's disruptive effect

b) Appendix II – List of digital services

c) Appendix III – List of competent authorities.

Harmonization with the EU legislation

Article 2

(1) This Act transposes into the legislation of the Republic of Croatia the 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 L 194, 19 July 2016).

(2) This Act ensures the implementation of the Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact (OJ L 26/48, 31 January 2018 – hereinafter referred to as: Commission Implementing Regulation).

Application

Article 3

(1) This Act applies to operators of essential services, whether they are public or private entities, regardless of the state of their head office, their size, structure or ownership.

(2) Digital service providers are subject to competences and authorities stipulated by this Act if they either have their head office or their representative on the territory of the Republic of Croatia and under the condition that such provider does not represent a micro or small sized enterprise as defined by the Act stipulating the basis for the implementation of economic incentives aimed towards development, restructuring and market adaptation of small sized enterprises.

Relationship with other legislation

Article 4

(1) If, in the implementation of this Act, classified information is generated or used or personal information is processed, special legislation on the protection of such information shall be applied.

(2) If there are measures stipulated by a special Act for a specific sector referred to in the List in Appendix I of this Act, which fulfill the requirements laid down by this Act in their content and objective, or represent stricter requirements, such provisions of the special Act shall apply to the operators of essential services belonging to this sector.

Definitions

Article 5

Particular notions within the meaning of this Act shall have the following meaning:

1) cybersecurity – is the system of organizational and technical activities and measures aimed at reaching the authenticity, confidentiality, integrity and availability of information, as well as network and information systems in cyberspace

2) cyberspace – is a virtual space where communication between network and information systems takes place and includes all network and information systems, regardless of their connection to the Internet

3) network and information system – is (a) an electronic communications network as defined by the Act stipulating the electronic communications area; (b) any device or group of interconnected or related devices, one or more of which, performs automatic processing of digital data pursuant to a program or (c) digital data stored, processed, retrieved or transmitted by elements described under (a) and (b) for the purposes of their operation, use, protection and maintenance

4) security of network and information system – is the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems

5) national strategy on cybersecurity – is a framework providing strategic objectives and priorities on cybersecurity at national level

6) competent authorities – are competent sectoral authorities, single national point of contact, competent CSIRTs and technical compliance evaluation authorities,

7) operator of essential services – is a public or private entity which meets the criteria laid down in Article 6 of this Act

8) digital service provider – is any private entity providing a digital service in the European Union referred to in the List from Appendix II of this Act

9) public entities – are government authorities, other state authorities, local and regional self-government bodies, legal persons with public authority or performing public service

10) private entities – are individuals or legal entities providing or offering services

11) head office – is a permanent place of business where operator or service provider manages their activities for an indefinite period of time

12) representative – is any individual or legal entity with a head office in the Republic of Croatia, who has been duly appointed by the digital service provider with a head office outside of the European Union to act on their behalf and whom the competent sectoral authority or competent CSIRT may contact instead of the digital service provider liable pursuant to this Act

13) incident – is any event having an actual adverse effect on the security of network and information systems

14) incident handling – are all the procedures supporting the detection, analysis and containment of an incident and the response thereto

15) risk – is any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems

16) Internet exchange point (IXP) – is a network facility which enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of Internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the Internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic

17) domain name system (DNS) – is a hierarchical distributed naming system in a network which refers queries for domain names

18) DNS service provider – is a public or private entity which provides DNS services on the Internet

19) top-level domain name registry – are public or private entities which administer and operate the registration of Internet domain names under a specific top-level domain (TLD)

20) online marketplace – is a digital service that allows consumers and/or traders, as respectively defined by the Act regulating the alternative dispute resolution for consumer disputes, to conclude online sales or service contracts with traders either on the online marketplace's website or on a trader's website that uses computing services provided by the online marketplace

21) online search engine – is a digital service that allows users to perform searches of, in principle, all websites or websites in particular language on the basis of a query on any subject in the form of a keyword, phrase or other input, and returns links in which information related to the requested content can be found

22) cloud computing service – is a digital service that enables access to a scalable and elastic pool of shareable computing resources, services and applications

23) member state – is a state member of the European Union

24) qualified auditor – is an individual or legal entity who is accredited for auditing the security of network and information systems by the appropriate standardization organization, which publishes or provides standards that are applicable, within the framework of the implementation of this Act, to a certain operator of essential services or digital service provider

25) security audit of network and information systems – are procedures performed by a qualified auditor in order to assess the harmonization of established processes of network and information systems management and documented security policies with the requirements stipulated by this Act

26) CSIRT – is an abbreviation for Computer Security Incident Response Team, the competent authority for incident prevention and protection, whereas in the Republic of Croatia the abbreviation CERT (Computer Emergency Response Team) is also used.

PART II

OPERATORS OF ESSENTIAL SERVICES AND DIGITAL SERVICES

Identification of operators of essential services

Article 6

Individual public or private entity (hereinafter referred to as: entity) shall be identified as the operator of essential services if:

a) an entity provides one of the essential services from the List in Appendix I of this Act (hereinafter referred to as: essential service)

b) the provision of essential service by said entity depends on network and information systems and

c) an incident would have significant disruptive effect on the provision of essential service.

Identification procedure

Article 7

(1) Competent sectoral authorities shall perform the identification procedure of operators of essential services by sectors as defined in the List from Appendix I of this Act, whereby:

a) the lists of all entities providing essential service are made

b) entities are selected based on the significance of the disruptive effect an incident would have on providing the essential service by said entity and

c) the evaluation of dependency of providing essential service on network and information systems is performed for all selected entities.

(2) The competent sectoral authority shall perform the identification procedure of operators of essential services regularly, in accordance with the market changes in the sector, but at least once every two years.

Determining the significance of incident's disruptive effect

Article 8

(1) When determining the significance of a disruptive effect that an incident would have on operators of essential services, the following criteria shall be taken into account:

– number and type of users to whom the entity provides service

– dependency of other sectors or areas on service provision

– market share of the entity providing service

– geographic spread of entity in providing service

– possible impact of the incident, in terms of its degree and duration, on economic and societal activities or public safety

– the importance of the entity for maintaining a sufficient level of essential service, taking into account the availability of alternative means for the provision of that service or

– other sectoral criteria such as the quantity of service provided, share in providing service or the assets of the entity.

(2) The criteria referred to in paragraph 1 of this Article as well as thresholds, if defined, shall be applied in the process of identification of operators of essential services, as divided in accordance with essential service as defined in the List in the Appendix I of this Act.

(3) If the entity providing essential service meets the criteria from the List in the Appendix I of this Act and reaches the threshold, when defined by the List, the estimate of significance of incident's disruptive effect shall be made on essential service provision by that entity and said entity shall be singled out for determining the dependency of essential service provision on network and information systems.

Determining the dependency on network and information system

Article 9

(1) In case it is established that the entity referred to in Article 8, paragraph 3 of this Act uses a network and information system for support in providing essential services and that the cease of operation or malfunction of such system may cause disruptions in providing service or in some other way adversely affect the quality and/or volume of service, the competent sectoral authority shall adopt a decision on identifying such entity as operator of essential services.

(2) Notwithstanding the provisions of paragraph 1 of this Article, the competent sectoral authority may adopt a decision on identifying the entity as operator of essential services, regardless of the criteria from the List in Appendix I of this Act, if during the identification process it is determined that the entity provides essential service in two or more member states and that the entity's dependency on network and information system in providing service may have adverse cross border effect on service providing continuity.

(3) Competent sectoral authority shall, in order to determine the critical cross border effect referred to in paragraph 2 of this Article, in cooperation with the single national point of contact, cooperate with the competent national authority of the member state involved.

Identification notification

Article 10

Competent sectoral authority shall forward to the identified operator of essential services the notification of decision referred to in Article 9 of this Act within 8 days from its adoption.

Submitting information necessary for identification of operators of essential services

Article 11

(1) Each entity providing any of the essential services shall, upon request, submit to the competent sectoral authority the information necessary for the procedure of identifying operators of essential services.

(2) The request referred to in paragraph 1 of this Article shall state the purpose of request, the information necessary and the deadline for submitting the information.

(3) Entities, where changes occur in relation to the information submitted in accordance with paragraph 2 of this Article, shall submit to the competent sectoral authority the notification of such changes if they might affect the status of the entity during the process of identification of operators of essential services.

(4) Notifications referred to in paragraph 3 of this Article shall be submitted within 7 days from the day when the change occurred or was introduced.

List of operators of essential services

Article 12

(1) Based on the decision referred to in Article 9 of this Act, competent sectoral authorities shall draw up, review and update the list of operators of essential services by sectors referred to in the List in Appendix I of this Act.

(2) Competent sectoral authorities shall notify the single national point of contact about the number of identified operators of essential services in an individual sector, also stating their importance for the sector.

Digital services

Article 13

Digital services, on whose providers this Act applies, shall be identified in the List in Appendix II of this Act.

PART III

MEASURES FOR ACHIEVING A HIGH LEVEL OF CYBERSECURITY OF OPERATORS OF ESSENTIAL SERVICES AND DIGITAL SERVICE PROVIDERS

Obligation to implement measures

Article 14

(1) Operators of essential services and digital service providers shall, in order to ensure business continuity in providing services, implement the measures for achieving a high level of cybersecurity of their services.

(2) The measures referred to in paragraph 1 of this Article shall include at least the following:

– technical and organizational measures for risk management, taking into consideration state of the art technical achievements used within the framework of best security practices in the cybersecurity area and

– measures aimed at preventing and mitigating the effect of incidents on the security of network and information systems.

Risk management measures for operators of essential services

Article 15

Operators of essential services shall implement technical and organizational measures for risk management, which shall include measures aimed at:

– determining the risk of incidents

– preventing, detecting and handling incidents and

– mitigating the effect of incidents to the least possible measure.

Risk management measures for digital service providers

Article 16

Digital service providers shall, while implementing technical and organizational measures for risk management, especially take into account the following:

– the security of systems and facilities

– incident handling

– business continuity management

– monitoring, auditing and testing

– compliance with international standards.

Scope of measures' implementation

Article 17

(1) Operators of essential services shall implement the measures for achieving a high level of cybersecurity in relation to network and information system, or its part, which was determined during the process of identification of operator of essential services to be crucial in providing the essential service of the respective entity.

(2) Digital service providers shall implement the measures for achieving a high level of cybersecurity in relation to network and information system that supports their digital service.

Measures' implementation according to risk assessment

Article 18

Operators of essential services and digital service providers shall implement the measures for preventing and mitigating the effects of incidents in proportion to the risk posed to their network or information system.

Responsibility for measures' implementation

Article 19

Operators of essential services and digital service providers shall implement the measures for achieving a high level of cybersecurity whether they manage and/or maintain their network and information systems by themselves or outsource it to an external service provider.

Stipulating the measures

Article 20

(1) The measures for achieving a high level of cybersecurity of operators of essential services and means for their implementation shall be stipulated by the Regulation adopted by the Government of the Republic of Croatia (hereinafter referred to as: the Government).

(2) The measures for achieving a high level of cybersecurity of digital service providers shall be implemented in accordance with the Commission Implementing Regulation referred to in Article 2, paragraph 2 of this Act.

PART IV

INCIDENT NOTIFICATION

Responsibility for notification

Article 21

(1) Operators of essential services and digital service providers shall, without undue delay, notify the competent CSIRT on incidents which have a significant impact on the continuity of services they provide.

(2) Where an incident on digital service provider's network and information system had a significant impact on the provision of any essential service, the operator of essential services shall notify the competent CSIRT about such incident.

(3) The responsibility for notification referred to in this Article shall include the incidents on network and information systems referred to in Article 17 of this Act.

Criteria to identify the impact of incidents

Article 22

(1) The criteria to identify incidents with significant impact on providing essential services shall be stipulated by the Government Regulation referred to in Article 20, paragraph 1 of this Act.

(2) The criteria to identify incidents with significant impact on providing digital services shall be stipulated by the Commission Implementing Regulation referred to in Article 2, paragraph 2 of this Act.

Notification of incidents

Article 23

The content of the notification of incidents referred to in Article 21 of this Act, the means of its provision and other issues relevant for handling such notifications shall be stipulated by the Government Regulation referred to in Article 20, paragraph 1 of this Act.

Informing the public about the incident

Article 24

(1) The competent CSIRT may, after previously consulting the operator of essential services and the competent sectoral authority, inform the public about individual incidents which have a significant impact on the continuity of service provided by the operator, where public awareness is necessary in order to prevent the spread of incident or the increase of its impact or to deal with an ongoing incident.

(2) The competent CSIRT and, if necessary, CSIRTs of other affected member states, may inform the public about individual incidents which have a significant impact on the continuity of individual digital service or may ask the digital service provider to do so, where the publication of the information about incidents is in public interest, especially if it is necessary in order to prevent the spread of incident or the increase of its impact or to deal with an ongoing incident.

PART V

COMPETENT AUTHORITIES

Competent sectoral authorities

Article 25

(1) Competent sectoral authorities shall be stipulated by the List in Appendix III of this Act.

(2) Competent sectoral authorities shall:

– identify operators of essential services in accordance with this Act

– perform oversight of operators of essential services and digital service providers in implementing the measures for achieving a high level of cybersecurity and fulfilling other obligations stipulated by this Act

– mutually cooperate and exchange experiences in the course of the implementation of this Act

– cooperate and exchange relevant information with other competent authorities referred to in this Act

– cooperate and exchange relevant information with the authority competent for personal data protection, when personal data is in danger due to the incident in network and information system of the operator of essential services or digital service provider, or with law enforcement authorities, when such incident is a result of criminal activities.

Oversight

Article 26

(1) The oversight of operators of essential services shall be performed once every two years.

(2) The oversight of operators of essential services shall be performed even before the expiration of deadline referred to in paragraph 1 of this Article, when the competent sectoral authority establishes or receives information indicating that the operator of essential services does not fulfill their obligations stipulated by this Act.

(3) The oversight of digital service providers shall be performed only after the competent sectoral authority receives information indicating that the digital service provider does not act in accordance with the Commission Implementing Regulation referred to in Article 2, paragraph 2 of this Act and/or the obligations stipulated by this Act.

(4) Competent sectoral authority for digital service providers shall perform oversight with the support of the competent technical compliance evaluation authority and the competent CSIRT.

Obligations of operators of essential services and digital service providers within the oversight framework

Article 27

(1) Operators of essential services and digital service providers shall, upon request, within the oversight framework, provide the competent sectoral authority with the following:

– information necessary to evaluate the security level of their network and information systems, including documented security policies, and

– proof of effective implementation of security measures.

(2) Effective implementation of security measures shall be proven either by audit results of security of network and information systems performed by a qualified auditor or by compliance evaluation of network and information systems provided by a technical compliance evaluation authority.

(3) The request referred to in paragraph 1 of this Article shall include the purpose of the request, the information necessary for the competent sectoral authority to perform oversight and the deadline for the provision of information.

(4) Operators of essential services and digital service providers shall, within the oversight framework, upon its request, provide the competent sectoral authority with direct access to their facilities and systems used for support in providing essential or digital services.

(5) The competent sectoral authority may perform the oversight of digital service providers with head office or representatives in the Republic of Croatia, and whose network and information systems are located in another members state or more member states, in cooperation with the competent authorities of the respective member states.

Subject of oversight

Article 28

(1) Within the oversight framework, the competent sectoral authorities shall control the regularity of implementation of the stipulated:

– measures for achieving a high level of cybersecurity

– obligations related to notifications about incidents and

– other actions in accordance with the request of competent authorities submitted in accordance with this Act or another regulation adopted on the basis of this Act.

(2) During oversight, the competent sectoral authorities shall:

– issue a binding instruction to the operator of essential services, when it is established that:

a) they have not implemented the measures for achieving a high level of cybersecurity and/or have not implemented other obligations stipulated by this Act or

b) there are deficiencies in the implementation of measures or obligations from this Act

– issue orders to digital service providers to eliminate any established non-compliance of the Commission Implementing Regulation referred to in Article 2, paragraph 2 of this Act and/or provisions of this Act

– submit a motion for indictment.

(3) Competent sectoral authorities shall, in acts referred to in paragraph 2, subparagraph 1 and 2 of this Article define the deadline for proceedings.

Oversight implementation

Article 29

Oversight shall be implemented by inspectors, controllers and supervisors, in accordance with the competences defined in the regulations on the structure and scope of work of respective authorities and other regulations stipulating their competences.

Single national point of contact

Article 30

Single national point of contact shall:

– provide information to the European Commission which enables the evaluation of effectiveness of the implementation of measures from this Act and regulations adopted on the basis of this Act, in accordance with the requirements stipulated by the Regulation referred to in Article 2 of this Act

– participate in the work of Cooperation Group, established in order to support and facilitate strategic cooperation and the exchange of information among member states and to develop trust and security at the European Union level in cybersecurity area,

– once per year submit to the Cooperation Group a summary report on received incident notifications, including the number of notifications and nature of incidents reported and actions implemented in accordance with Article 21 and Article 32, paragraph 1, points 8, 10 and 11 of this Act, except for the sector of business services for state authorities

– based on the request by the competent CSIRT, forward the incident notifications referred to in Article 21 of this Act to the single points of contact of other member states affected, except for the sector of business services for state authorities

– draw up guidelines on the content of notification, means and deadlines for informing the single national point of contact on the number of identified operators of essential services and their importance and incident notifications

– take care of the need to develop and harmonize the national cybersecurity strategy with the objectives of this Act and the requirements of the European Union in the cybersecurity area

– cooperate with other competent authorities referred to in this Act

– when necessary, consult and cooperate with the authority competent for personal data protection and law enforcement authorities.

Article 31

Single national point of contact is the Office of the National Security Council.

Competences of the competent CSIRT

Article 32

(1) The competent CSIRT at sectoral level, in accordance with the list of competences from Appendix III of this Act, shall:

– monitor incidents

– provide early warnings and announcements and inform about risks and incidents

– perform dynamic analysis of risks and incidents and provide a situation overview in the sector

– perform regular vulnerability assessments of network and information systems of operators of essential services and digital service providers

– receive incident notifications

– upon request of the operators of essential services or digital service providers analyze and respond to incidents

– circumstances permitting, after receiving the incident notification, provide the operator of essential services with the relevant information on further proceedings following their notification, especially the information that could be beneficial for the effective incident handling

– adopt guidelines for harmonizing and improving the implementation of incidents notification referred to in Article 21 of this Act

– inform the competent sectoral authority about incidents referred to in Article 21 of this Act

– in cooperation with the competent sectoral authority, define cross border impact of incidents referred to in Article 21 of this Act

– inform the single national point of contact on incidents referred to in Article 21 of this Act, in accordance with their guidelines

– provide the single national point of contact with the information on the main elements of incident handling procedures implemented

– inform the competent CSIRT of another member state affected or more of them about the incident referred to in Article 21 of this Act on the network and information system of operator of essential

services, if the incident has significant impact on the continuity of essential services in that member state

– inform the competent CSIRT of another member state affected or more of them about the incident referred to in Article 21 of this Act on the network and information system of digital service providers if the incident affects two or more member states

– cooperate with other CSIRTs on the national and international level

– participate in CSIRTs Network on the European Union level, which was established in order to develop confidence and trust between member states and to promote swift and effective operational cooperation

– promote the adoption and implementation of common or standardized practices for handling incidents and risks as well as plans for classifying incidents, risks and information.

(2) Operators of essential services and digital service providers shall cooperate with the competent CSIRT and exchange all the information necessary for incident handling.

(3) The competent CSIRT, in the performance of its tasks stipulated by this Act, may not be held responsible for the damage caused by an incident on network and information systems of operators of essential services and digital service providers.

Ensuring the conditions for performance of competent CSIRT's tasks

Article 33

The competent CSIRT shall:

– ensure a high level of availability of its communication services by avoiding single points of failure, with the availability of means of two-way communication and clearly specified and well known communication channels to the constituency and cooperative partners

– place their premises and supporting information systems in secure sites and

– ensure business continuity by:

a) being equipped with the appropriate system for managing requests and routing them, in order to facilitate handover

b) being adequately staffed in order to appropriately ensure availability at all times

c) relying on infrastructure whose continuity is ensured and has redundant systems and backup work space for such purposes.

Technical compliance evaluation authority

Article 34

(1) Technical compliance evaluation authority shall perform periodical evaluation of measures referred to in Article 14 of this Act, which were implemented over the security of network and information systems of operators of essential services and digital service providers, if the security audit of network and information systems is not performed by a qualified auditor.

(2) Technical compliance evaluation authorities shall be defined by the List in Appendix III of this Act.

Request for compliance evaluation

Article 35

(1) Technical compliance evaluation authority shall perform the evaluation referred to in Article 34 of this Act upon request by the competent sectoral authority or the operators of essential services or digital service providers themselves.

(2) The competent sectoral authority shall submit the request referred to in paragraph 1 of this Article when it is established that the security audit of network and information systems of individual operator of essential service or digital service provider has not been implemented or was not done by a qualified auditor.

(3) Operator of essential service or digital service provider may submit the request for compliance evaluation when there is no obligation to audit the subject in accordance with a special regulation.

Provision of information during compliance evaluation

Article 36

(1) Operators of essential services and digital service providers shall, upon request, provide the technical authority for compatibility evaluation the information necessary to evaluate the security level of their network and information systems and enable access to their facilities and systems used for support in performing essential or digital services.

(2) The request referred to in paragraph 1 of this Article shall include the purpose of the request, the information necessary and the deadline for providing the information.

Report on compliance evaluation

Article 37

(1) Technical compliance evaluation authority, after having performed the evaluation referred to in Article 34 of this Act, shall draft a report on the measures for reaching a high security level of network and information systems, which shall include:

– compliance evaluation, if established that the operator of essential service or digital service provider effectively implements the measures for achieving the high level of cybersecurity or

– corrective measures for the effective implementation of measures for achieving a high level of cybersecurity, with the deadline for their implementation.

(2) Technical compliance evaluation authority shall submit the report referred to in paragraph 1 of this Article, without delay, to the competent sectoral authority and operator of essential services or digital service provider.

Final report on compliance evaluation

Article 38

(1) Operator of essential services, as well as digital service provider, shall, within the prescribed timeframe, implement the corrective measures and, without delay, notify the technical compliance evaluation authority.

(2) Technical compliance evaluation authority shall, after the receipt of notification referred to in paragraph 1 of this Article, as well as in case of non-implementation or incomplete implementation of corrective measures, draft the final report on the evaluation referred to in Article 34 of this Act, which shall be submitted to the competent sectoral authority for oversight purposes.

Notification on disabling or hindering the implementation of compliance evaluation

Article 39

If the operator of essential services or digital service provider fails to enable or without justification delays or hinders the implementation of evaluations referred to in Article 34 of this Act, the technical compliance evaluation authority shall, without delay, inform the competent sectoral authority.

PART VI

PROTECTION OF INFORMATION

Article 40

(1) The lists of operator of essential services, as well as all other information generated in the course of the implementation of this Act, shall only be used for the purpose of fulfilling the obligations stipulated by this Act.

(2) The list and information referred to in paragraph 1 of this Article shall constitute the information in relation to which the access right may be restricted to information user, depending on the results of the test of proportionality and public interest, which is implemented in accordance with the provisions of a special act on the right of access to information.

(3) When exchanging the information referred to in paragraph 1 of this Article, the competent authorities shall take into consideration the need to restrict access to information when it is necessary in order to prevent, detect, perform investigations and criminal proceedings.

Article 41

Competent authorities referred to in this Act shall handle the information of operators of essential services and digital service providers in accordance with the provisions on confidentiality, if stipulated by special regulations on the protection of such information.

PART VII

PENALTIES

Article 42

(1) A fine in the amount between HRK 150 000.00 and HRK 500 000.00 shall be imposed for the minor offence on the legal entity – operator of essential service, who:

– does not act in accordance with the binding instruction of the competent sectoral authority referred to in Article 28 paragraph 2, subparagraph 1 of this Act

– fails to submit or delays without justification the provision of incident notification referred to in Article 21 of this Act.

(2)) A fine in the amount between HRK 50 000.00 and HRK 150 000.00 shall be imposed for the minor offence referred to in paragraph 1 of this Article on the individual craftsman or other self-employed individual.

(3) A fine in the amount between HRK 15 000.00 and HRK 50 000.00 shall be imposed for the minor offence referred to in paragraph 1 of this Article on the responsible person in the legal entity and the responsible person in the public entity.

Article 43

(1) A fine in the amount between HRK 150 000.00 and HRK 500 000.00 shall be imposed for the minor offence on the legal entity - digital service provider, who:

– does not act in accordance with the instruction of the competent sectoral authority referred to in Article 28, paragraph 2, subparagraph 2 of this Act

– fails to submit or delays without justification the notification of incidents referred to in Article 21 of this Act.

(2) A fine in the amount between HRK 50 000.00 and HRK 150 000.00 shall be imposed for the minor offence referred to in paragraph 1 of this Article on the individual craftsman or other self-employed individual.

(3) A fine in the amount between HRK 15 000.00 and HRK 50 000.00 shall be imposed for the minor offence referred to in paragraph 1 of this Article on the responsible person in the legal entity and the responsible person in the public entity.

Article 44

(1) A fine in the amount between HRK 50 000.00 and HRK 100 000.00 shall be imposed for the minor offence on the legal entity– operator of essential service and digital service provider, who:

– refuses to act or fails to act without any justification upon request referred to in Article 27 of this Act

– fails to enable or without justification delays or hinders the action of the technical compliance evaluation authority referred to in Article 35, paragraph 2 of this Act.

(2) A fine in the amount between HRK 20 000.00 and HRK 50 000.00 shall be imposed for the minor offence referred to in paragraph 1 of this Article on the individual craftsman or other self-employed individual.

(3) A fine in the amount between HRK 10 000.00 and HRK 25 000.00 shall be imposed for the minor offence referred to in paragraph 1 of this Article on the responsible person in the legal entity and the responsible person in the public entity.

Article 45

(1) A fine in the amount between HRK 15 000.00 and HRK 50 000.00 shall be imposed for the minor offence on the legal entity – entity providing one of the essential services, who:

– does not act upon request of the competent sectoral authority for the provision of information referred to in Article 11, paragraph 1 of this Act

– does not provide the notifications of changes of deadlines referred to in Article 11, paragraph 4 of this Act.

(2) A fine in the amount between HRK 5 000.00 and HRK 25 000.00 shall be imposed for the minor offence referred to in paragraph 1 of this Article on the individual craftsman or other self-employed individual.

(3) A fine in the amount between HRK 2 000.00 and HRK 20 000.00 shall be imposed for the minor offence referred to in paragraph 1 of this Article on the responsible person in the legal entity and the responsible person in the public entity.

PART VIII

TRANSITIONAL AND FINAL PROVISIONS

Article 46

The Regulation referred to in Article 20 paragraph 1 of this Act shall be adopted by the Government of the Republic of Croatia within 30 days from the date when this Act enters into force.

Article 47

(1) Competent sectoral authorities shall identify the operators of essential services within 90 days from the day when this Act enters into force.

(2) Competent sectoral authorities shall submit the notification referred to in Article 12 paragraph 2 of this Act to the single national point of contact within 120 days from the day when this Act enters into force.

Article 48

(1) Operators of essential services shall implement the measures for achieving a high level of cybersecurity within a year from the day of delivery of the notification referred to in Article 10 of this Act.

(2) Operators of essential services shall start submitting the notifications referred to in Article 21 of this Act within 30 days from the day of delivery of the notification referred to in Article 10 of this Act.

Article 49

(1) Digital service providers shall harmonize with the requirements stipulated by the Commission Implementing Regulation referred to in Article 2 paragraph 2 of this Act within the deadline stipulated by that Regulation.

(2) Digital service providers shall start submitting notifications referred to in Article 21 of this Act within 120 days from the day when this Act enters into force.

Article 50

This Act shall enter into force 8 days following its publication in the Official Gazette.

Class: 022-03/18-01/48

Zagreb, 6 July 2018

THE CROATIAN PARLIAMENT

The President
of the Croatian Parliament

Gordan Jandroković, m. p.

APPENDIX I

LIST OF ESSENTIAL SERVICES WITH CRITERIA AND THRESHOLDS FOR DETERMINING THE SIGNIFICANCE OF THE INCIDENT'S DISRUPTIVE EFFECT

Sector	Subsector	Essential service	Criteria for determining the incident's disruptive effect	Thresholds for determining the incident's disruptive effect
Energy	Electricity	Production of electricity	Installed power of generating capacity	300 MW
		Transmission of electricity	No exception	–
		Distribution of electricity	Electricity supply interruption	More than 100 000 metering points
			Dependency of other activities or areas on the provision of service	Distribution for: ☐ hospitals ☐ airports and air traffic controls ☐ banking facilities with data centers ☐ police directorates ☐ military facilities ☐ active water wells and management centers ☐ facilities of telecommunication systems operators ☐ facilities of the security and

				intelligence system authorities, ☐ facilities of professional fire brigades, ☐ facilities of National Protection and Rescue Directorate (112 Service) or ☐ facilities defined as national critical infrastructure
	Oil	Oil transmission pipelines	No exception	–
		Oil production	Oil produced on the single oil field in tons per year	50 000 tons per year
		Production of petroleum products	Petroleum products produced by a single refinery in tons per year	Motor gasoline: 200 000 tons per year Diesel fuel: 200 000 tons per year Gas oils: 100 000 tons per year
		Storage of oil and petroleum products	Total oil storage capacity of a single terminal in m3	1 000 000 m3
			Total petroleum products storage capacity in a single storage (at the same location) in m3	60 000 m3
	Gas	Distribution of gas	Number of end users connected to the distribution system	More than 100 000 metering points

		Transport of gas	No exception	
		Storage of gas	Gas consumption in the Republic of Croatia in kWh	25 % of gas consumption in the Republic of Croatia in the previous year
		LNG importation and offloading	LNG regasification capacity in m3/h	More than 500 000 m3/h
		Production of natural gas	Annual gas production transmitted to the transport system at individual entry, in kWh	1 000 000 kWh
Transport	Air transport	Air transport of passengers and cargo	Passenger share of a single air carrier in any national airport with annual passenger traffic of more than 2 000 000 (core airport)	Air carrier with a share of more than 30 % at core airport
		Managing airport infrastructure, including ancillary installations contained within airports	Total annual passenger traffic of a single airport	More than 2 000 000 passengers
		Air traffic control	Openness of flight information region Zagreb (FIR Zagreb) – no exception	–
			Number of operations per year	Total of 500 000 operations for FIR Zagreb
	Rail transport	Managing and maintaining rail	Rail infrastructure manager for public transport – no exception	

		infrastructure, including traffic management and control-command and signaling subsystem		
		Rail transport services of goods and/or passengers	Number of units (trains)	20 per day
		Managing service facilities and providing services in service facilities	Number of units (trains)	20 per day
		Providing additional services necessary for rail transport of goods or passengers	Number of units (trains)	20 per day
	Water transport	Maritime traffic monitoring (VTS service)	Annual number of arrivals of international navigation vessels	minimum 4 000
			Annual number of travel of domestic navigation vessels, including coastal liner traffic	minimum 200 000
		Maritime radio services	Annual number of arrivals of international navigation vessels	minimum 4 000

			Annual number of travel of domestic navigation vessels, including coastal liner traffic	minimum 200 000
		Managing maritime security facilities	No exception	–
		International and/or domestic passenger transport	Annual number of passengers	1 000 000
	Water transport	Cargo loading and offloading in ports in international and domestic traffic	Annual cargo quantity in tons	2 500 000
		Transport of passengers, cargo and vehicles in inland maritime waters and territorial sea of the Republic of Croatia on previously defined lines according to public journey schedule and price list	Number of users	15 % of total passengers and/or vehicles per year
			Market share	Minimum 15 % of market share
		Tracking and locating vessels in	Number of vessels in inland waterways in the Republic of Croatia per year	100

		inland waterways		
		Notifications to vessels in inland waterways	Number of notifications issued per year	100
		Access to electronic navigation charts in inland waterways	Coverage of inland waterways in the Republic of Croatia	Coverage of 500 river km
		Hull data base in inland waterways	Number of vessels entered into the data base per year	50
		International electronic reporting in inland waterways	Number of ERI messages sent to RIS centres per day	50
	Road transport	Public passenger transport	Number of transport units	100
			Annual number of passengers	5 000 000
		Road infrastructure usage	Road manager on TEN – T network – no exception	–
			Number of vehicles on the main road leading to the center of town with more than 35 000 inhabitants	20 000 annual average daily traffic
			Geographic coverage of service usage	Territory of an entire state or town with more than 35 000 inhabitants

		Traffic flow management or intelligent transport systems (ITS)	Center for traffic control and management 24/7– no exception	
			Center for informing the drivers on traffic situation 24/7 – no exception	
			Number of traffic lights in the system	100
			Geographic coverage of service usage	Territory of an entire state or town with more than 35 000 inhabitants
Banking		Payment services	Globally systemically important credit institutions and other systemically important credit institutions	–
Financial market infrastructure		Trading venue services	No exception	–
		Central counterparties services (CCP)	No exception	–
Health sector		Primary health care	Croatian central health information system – no exception	–
			Coverage of primary health care providers by an approved program solution	40 %
			Number of out-of-hospital emergency interventions per county per year	70 000
			Number of health professionals employed in a medical center	500

			Health VPN network HealthNet – no exception	–
		Secondary health care	Coverage of secondary health care providers by an approved program solution	40 %
			Number of performed health procedures, check-ups or examinations per year	1 000 000
			Number of health professionals employed in a general hospital	800
		Tertiary health care	Number of beds in stationary part of clinical hospital center	900
			Number of beds in stationary part of clinical hospital	300
			Number of beds in stationary part of a clinic	80
		Transfusion medicine and organ transplantation	Number of whole blood doses collected per year	100 000
			Number of organ donors per million inhabitants per year	30
			Number of transplantations per million inhabitants per year	80
		Health insurance and cross border health care	Number of persons insured by compulsory health insurance	4 000 000
			Number of persons insured by supplementary health insurance	2 000 000

			Number of status check queries regarding compulsory and supplemental health insurance per day	100 000
			Number of European Health Insurance Cards (EHIC) issued per year	100 000
		Food safety	Central information system of the sanitary inspection – no exception	
		Protection against hazardous chemicals	Number of safety data sheets checked and entered into the Safety Data Sheet Registry per year	9 000
			Number of hazardous chemicals collected and entered into the Registry of hazardous chemicals imported on the territory of the Republic of Croatia per year	3 500
		Distribution and security of medicines and medical products	Number of medicines (including vaccines) placed on the market in the Republic of Croatia	3 000
			Number of medical products (different risk classes) placed on the market in the Republic of Croatia	250 000
			Number of inhabitants / insured persons per number of distribution centers	330 000

		Control over health care status of the population and human resources in health care by managing public health care registries	National public health care information system – no exception	–
Drinking water supply and distribution		End users' supply	Water quantity distributed	10 000 000 m³ per year
Digital infrastructure		DNS service for .hr TLD	No exception	–
		Domain name registry for .hr TLD	No exception	–
		System for registration and administration of secondary domain	Entity providing essential service, with a domain registered in registry and recognizing the dependence of its service on the DNS system	–
			Number of registered domains	20 % of total number of domains registered (within .hr and com.hr)
		IXP service	Number of connected members	More than15
Business services for		Services in e-citizen system	Number of individual service users	100 000

state authorities			Service availability exclusively as an electronic service	No alternative way of using the service
		Business services for state budget users	Number of institutions not connected within a sector	10

APPENDIX II

LIST OF DIGITAL SERVICES

1. Online marketplace
2. Online search engine
3. Cloud computing services

APPENDIX III

LIST OF COMPETENT AUTHORITIES

Single national point of contact – Office of the National Security Council

Essential services sector	Competent sectoral authority	CSIRT	Technical compliance evaluation authority
Energy	State administration authority competent for energy	Information Systems Security Bureau	Information Systems Security Bureau
Transport	State administration authority competent for transport	Information Systems Security Bureau	Information Systems Security Bureau
Banking	Croatian National Bank	National CERT	–
Financial markets infrastructure	Croatian Financial Services Supervisory Agency	National CERT	–
Health sector	State administration authority competent for health sector	Information Systems Security Bureau	Information Systems Security Bureau
Drinking water supply and distribution	State administration authority competent for water resources	Information Systems Security Bureau	Information Systems Security Bureau
Digital infrastructure	Central State Office for the Development of Digital Society	National CERT	Croatian Academic and Research Network– CARNET
Business services for state authorities	Central State Office for the Development of Digital Society	Information Systems Security Bureau or National CERT *	Information Systems Security Bureau or National CERT **

Digital service providers	Competent sectoral authority	CSIRT	Technical compliance evaluation authority

	State administration authority competent for economy	National CERT	Information Systems Security Bureau

*Note: Competent CSIRT for Business services for state authorities Sector is the Information Systems Security Bureau, except for the areas within the competence of the state authority competent for science and education, University Computing Center (Srce) or CARNET, where the competent CSIRT is the national CERT.

**Note: Technical compliance evaluation authority for Business services for state authorities Sector is the Information Systems Security Bureau, except for the areas within the competence of the state authority competent for science and education, University Computing Center (Srce) or CARNET, where the technical compliance evaluation authority is the Croatian Academic and Research Network – CARNET.