LAW
on Information Security

„Official Gazette of Republic of Serbia“, No. 6 /16, 94/17 and77/19

I. GENERAL PROVISIONS

Subject matter

Article 1

This Law lays down protection measures against security risks in information and communication systems, liability of legal persons in the management and use of information and communication systems, and defines competent authorities for implementation of protection measures, coordination between protection factors and monitoring of proper application of the prescribed protection measures.

Definitions

Article 2

For the purposes of this Law, the following definitions apply:

1) *information and communication system (ICT system)* means a technological and organizational unit that includes:

(1) electronic communications networks within the meaning of the law governing electronic communications;

(2) devices or groups of interconnected devices, such that automatic processing of data is performed within the devices, or within at least one of the group of devices, using a computer program;

(3) data, handled, kept, processed, searched or transmitted by elements covered under subitems (1) and (2) of this item, for the purposes of their operation, use, protection or maintenance;

(4) organizational structure through which the ICT system is managed;

(5) all types of system and application software and software development tools;

2) *ICT system operator* means a legal entity, an authority, or an organizational unit of an authority that uses the ICT system in performing its activities, i.e. the activities within the scope of its competence;

3) *information security* means a set of measures that enable the protection of the information being handled through the ICT system from unauthorized access, as well as the protection of integrity, availability, authenticity and non-repudiation of such information, in order for the system to function as foreseen, when foreseen and under the control of authorized persons;

4) *secrecy* means a property indicating that information is not available to unauthorized *persons*;

5) *integrity* means the preservation of original content and completeness of information;

6) *availability* means a property indicating that the information is available and usable at the request of authorized persons whenever they need it;

7) *authenticity* means a property indicating that it is possible to verify and confirm that the information was created or sent by the person declared to have performed the operation concerned;

8) *non-repudiation* means the ability to prove that a particular operation was carried out or that a particular event occurred, so that it cannot be denied at a later stage;

9) *risk* means the possibility of violating information security, i.e. the possibility of violating secrecy, integrity, availability, authenticity or non-repudiation of information, or the possibility of violating proper functioning of the ICT system;

10) *risk management* means a systematic set of measures that includes planning, organizing and directing activities in order to ensure that the risks remain within prescribed and acceptable frameworks;

11) *incident* is any event that has a negative impact on security of network and information systems;

11a) *single system for receiving notifications* is an information system inspecting incident data in ICT systems of significant importance that may have a significant influence on distribution of information security;

12) *ICT system protection measures* means technical and organizational measures for managing the ICT system security risks;

13) *classified information* means any information that is determined and classified with a certain degree of secrecy in accordance with the regulations on information secrecy;

14) *ICT system dealing with classified information* means the ICT system that is determined for dealing with classified information in accordance with the law;

15) public–authority means a state authority, an autonomous province's authority, a local self-government unit's authority, an organization and another legal entity or natural person whom is confidred with the exercise of public powers;

16) *security service* means a security service within the meaning of the law regulating the foundations of the Republic of Serbia's security and intelligence system;

17) *independent ICT system operators* means the ministry in charge of defense affairs, the ministry in charge of internal affairs, the ministry in charge of foreign affairs and the security services;

18) *compromising electromagnetic radiation (CEMR)* means unintentional electromagnetic emissions when transmitting, processing or storing information, the receipt and analysis of which can disclose the contents of such information;

19) *crypto security* means an information security component encompassing crypto protection, management of crypto materials and development of crypto protection methods;

22) *crypto protection* means the application of methods, measures and procedures for the purpose of transforming data into a form that makes them inaccessible to unauthorized persons for a certain period of time or permanently;

21) *cryptographic product* means a software or a device by which crypto protection is carried out;

22) *crypto materials* means cryptographic products, data, technical documentation for the cryptographic products, as well as appropriate cryptographic keys;

23) *security zone* means a space or room where classified information is processed and stored, in accordance with the regulations on information secrecy;

24) *information assets* include the data located in files and databases, program code, configuration of hardware components, technical and user documentation, usage logs for hardware components, for data in files and databases and for running procedures, if the said logs are kept, in-house general acts, procedures, and the like.

25) *information society service* means a service as defined in the law governing electronic commerce;

26) *information society service provider* means a service provider as defined in the law governing electronic commerce.

Principles

Article 3

When planning and implementing the ICT system protection measures, the following principles shall be observed:

1) principle of risk management - selection of measures and level of their implementation shall be based on the risk assessment, the need for risk prevention and elimination of the consequences of the risk realized, including all types of extraordinary circumstances;

2) principle of comprehensive protection - the measures shall be implemented at all organizational, physical, technical and technological levels, as well as during the ICT system's entire life cycle;

3) principle of expertise and good practice - the measures shall be implemented in accordance with professional and scientific knowledge and experience in the field of information security;

4) principle of awareness and competence - all persons who effectively or potentially affect information security by their actions should be aware of the risk and possess the appropriate knowledge and skills.

Personal Data Processing

Article 3a

In the event of personal data processing while exercising powers or meeting obligations hereunder, regulations governing personal data processing shall be complied with.

Competent authority

Article 4

The state administration body responsible for the ICT system security shall be the ministry responsible for information security (hereinafter: the Competent authority).

Body for the Coordination of Information Security Affairs

Article 5

In order to achieve cooperation and harmonized performance of tasks in the function of improving information security, as well as initiating and monitoring preventive and other activities in the field of information security, the Government shall establish the Body for the Coordination of Information Security Affairs (hereinafter: the Coordination Body), as a coordination body of the Government, which shall include the representatives of ministries responsible for information security, defense, internal affairs, foreign affairs, justice, of security services, Office of the National Security Council and Classified Information Protection, General Secretariat of the Government, National Bank of Serbia, Centre for ICT System Security of Authorities and National Center for the Prevention of Security Risks in ICT Systems.

In the function of improving certain areas of information security, professional working groups of the Coordination Body shall be formed, which shall include the representatives of other public authorities, economy, academic community and non-governmental sector.

By a decision establishing the Coordination Body, the Government shall determine its composition, tasks, deadline for reporting to the Government, and other issues related to its

work.

II. SECURITY OF ICT SYSTEMS OF SPECIAL IMPORTANCE

ICT systems of special importance

Article 6

ICT systems of special importance are the systems that are used for:

1) the performance of tasks in public authorities;

2) the processing of special categories of personal data within the meaning of the law governing the protection of personal data,;

3) the performance of activities of general interest and other economic activities in the following areas:

(1) Energy:
- production, transmission and distribution of electricity;
- coal production and processing;
- production, processing, transport and distribution of oil and trade of oil and petroleum products;
- research, production, processing, transport and distribution of natural and liquid gas.

(2) Transport:
- railway, postal and air traffic;

(3) Health sector:
- health care

(4) Banking and financial markets:
- operations of financial institutions;
- management of data registry on obligations of natural and legal persons to financial institutions;
- management operations and activities related to the functioning of a regulated market;

5) Digital infrastructure:
- exchange of internet traffic;
- management of the national Internet domain registry and the naming system in a network (DNS systems)

(6) Public goods:
- use, management, protection and improvement of public goods (water, roads, mineral resources, forests, navigable rivers, lakes, riverbanks, spas, wildlife, protected areas);

(7) Information society services:
- information society services within the meaning of Article 2 point 25) of this law.

(8) Other areas:
- electronic communication;
- publication of an official gazette of the Republic of Serbia;
- management of nuclear facilities;
- production, trade and transport of weapons and military equipment;
- waste management;
- utility services;
- production and supply of chemicals.

4) In legal entities and institutions established by the Republic of Serbia, the autonomous province or local self-government units for the performance of activity referred to in item 3) above.

On the proposal of the ministry competent for information security, the Government shall determine the list of activities referred to in paragraph 1, item 3) of this Article.

Obligations of an operator of an ICT system of special importance

Article 6a

An operator of an ICT system of special importance in accordance with this law shall:

1) List the ICT system of special importance it operates in the registry of operators of ICT systems of special importance;

2) Undertake protection measures of ICT systems of special importance;

3) Adopt an act on the security of the ICT system;

4) Perform a check of compliance of implemented ICT system protection measures with the act on the security of the ICT system at least once a year;

5) Arrange its relationship with third parties in a manner that ensures that protection measures for that ICT system are undertaken in accordance with the law, if it entrusts its activities related to the ICT system of special importance to third parties;

6) Submit notifications of incidents having a significant impact on information security of the ICT system;

7) Supply statistical data on incidents in the ICT system.

Registry of operators of ICT systems of special importance

Article 6b

The competent authority shall establish and maintain the registry of operators of ICT systems of special importance (hereinafter referred to as: the registry) which shall include:

1) Name and registered office of an operator of an ICT system of special importance;

2) Name and surname, official e-mail address and official contact telephone of an administrator of an ICT system of special importance;

3) Name and surname, official e-mail address and official contact telephone of a responsible person for an ICT system of special importance.

4) Information on the type of ICT system of special importance, in accordance with Article 6 hereof.

Register can include other additional data on ICT systems of special importance, which shall be regulated by competent authority.

An operator of an ICT system of special importance shall list the ICT system of special importance it operates in the registry referred to in paragraph 1 above.

An operator of an ICT system of special importance shall submit to the competent authority the data referred to in paragraph 1 above no later than 90 days from the date of adoption of the regulation referred to in Article 6, paragraph 2 hereof, i.e. 90 days from the date of establishment of an ICT system of special importance.

The competent authority shall make available to the national center for the prevention of security risks in ICT systems (hereinafter referred to as: the national cert) the updated registry referred to in paragraph 1 above.

Protection measures for ICT systems of special importance

Article 7

The ICT system of special importance operator shall be responsible for the security of an ICT system and for the ICT system protection measures.

The protection measures for the ICT system shall ensure the prevention against incidents, i.e. the prevention and reduction of damages from incidents that threaten the exercise of authorities and performance of activities, especially within the provision of services to other persons.

Protection measures for ICT systems refer to:

1) establishment of an organizational structure, with determined tasks and responsibilities of employees, which provides information security management within the ICT system operator;

2) achieving the safety of remote work and use of mobile devices;

3) ensuring that persons using the ICT system or managing the ICT system are qualified for their work and understand their responsibility;

4) protection against risks arising from changes in work or termination of employment of persons employed by an ICT system operator;

5) identification of information assets and determination of responsibility for their protection;

6) classification of data so that the level of their protection corresponds to the importance of the data in accordance with the principle of risk management referred to in Article 3 of this
Law;

7) protection of data carriers;

8) restriction of access to data and means of data processing;

9) approving authorized access and prevention of unauthorized access to an ICT system and services provided by the ICT system;

10) determining the responsibility of users to protect their own means of authentication;

11) providing the appropriate use of crypto protection in order to protect data secrecy, authenticity and integrity;

12) physical protection of facilities, premises, rooms or zones where the ICT system assets and documents are located and where the data are processed in the ICT system;

13) protection against loss, damage, theft or any other form of endangering the safety of the assets constituting the ICT system;

14) ensuring the proper and safe operation of data processing facilities;

15) protection of data and means of data processing against malicious software;

16) protection against data loss;

17) storing the data on events that may be of significance for the security of the ICT system;

18) ensuring the integrity of software and operating systems;

19) protection against abuse of technical security weaknesses of the ICT system;

20) ensuring that the activities of the audit of ICT systems have as little impact on the functioning of the system as possible;

21) data protection in communication networks including devices and lines;

22) security of data transmitted within the operator of the ICT system, as well as between the operators of the ICT system and persons outside the operator of the ICT system;

23) compliance with information security requirements in the management of all phases of the life cycle of an ICT system or parts of the system;

24) protection of the data used for testing of the ICT system or parts of the system;

25) protection of the ICT system operator’s assets that are available to service providers;

26) maintaining the contracted level of information security and services provided, in accordance with the terms and conditions agreed with the service provider;

27) prevention and response to security incidents, which implies an adequate exchange of information on ICT system security vulnerabilities, incidents and threats;

28) measures that ensure the continuity of operation in extraordinary circumstances.

The Government, on the proposal of the Competent authority, shall closely regulate the protection measures for the ICT system, taking into account the principles referred to in Article 3 of this Law, national and international standards and standards applicable in the respective fields of work.

Act on security of ICT systems of special importance

Article 8

An operator of the ICT system of special importance shall be obliged to adopt an act on the security of the ICT system.

The act referred to in paragraph 1 of this Article shall determine the protection measures, and in particular the principles, method and procedures to achieve and maintain an adequate level of system security, as well as the powers and responsibilities related to the security and resources of the ICT system of special importance.

The act referred to in paragraph 1 of this Article must be in line with changes in the environment and in the ICT system itself.

The operator of the ICT system of special importance shall be obliged, independently or by employing external experts, to perform a check of compliance of the implemented ICT system measures with the act referred to in paragraph 1 of this Article at least once a year, and to draft a report thereof.

The detailed content of the act referred to in paragraph 1 of this Article, the manner of checking an ICT system of special importance, and the content of the report on the check shall be determined by the Government on the proposal of the Competent authority.

Entrusting the ICT system of special importance related activities to third parties

Article 9

An operator of the ICT system of special importance may entrust its activities related to the ICT system to third parties, in this case it shall be obliged to arrange its relationship with such parties in a manner that ensures that protection measures for that ICT system are undertaken in accordance with the law.

The activities referred to in paragraph 1 of this Article (hereinafter referred to as: "entrusted activities") shall include all activities involving the processing, keeping or access to data held by the operator of an ICT system of special importance, which relate to its operations, as well as the development activities, i.e. the maintenance of software and hardware components that its proper handling in the performance of tasks within its competence or provision of services directly depends on.

The third party referred to in paragraph 1 of this Article shall also include a business entity that has property and management relations with the operator of the ICT system of special importance (persons with interest, members of a group of companies to which that business entity belongs, etc.).

Entrustment of the activities shall be performed on the basis of a contract concluded between the operator of the ICT system of special importance and the person to whom these activities are entrusted or by a special regulation.

Article 10

Notwithstanding the provisions of Article 9 of this Law, if the activities related to the ICT system are entrusted based on a regulation, such regulation may otherwise regulate the obligations and responsibilities of the operator of the ICT system of special importance in relation to the entrusted activities.

Incident notification

Article 11

The operators of ICT systems of special importance shall submit notifications of incidents in ICT systems that can have a significant impact on information security breaches through the portal of the competent authority or the National CERT to the single system for receiving notifications on incidents which shall be maintained by the competent authority.

If bodies referred in paragraph 1 are notified on incident by other means, they enter incident data in the system referred to in paragraph 1.

Notwithstanding paragraph 1 of this Article, notifications of incidents shall be forwarded to the:

1) National Bank of Serbia, in the event of incidents in ICT systems referred to in Article 6, paragraph 1, item 3, subitem (4), indent onehereof;
2) regulatory body for electronic communications, in the event of incidents in ICT systems referred to in Article 6, paragraph 1, item 3, subitem 8), indent one hereof.

The National bank of Serbia, The Regulatory Body for Electronic Communications shall forward the notifications, referred to in paragraph 3 above, to the single system for receiving notifications of incidents in the manner referred to in paragraph 1 above.

After the incident notification, if incident is still in progress, operators inform the body to whom incident is reported on important events and taken activities until the end of incident.

Operators of ICT system of special importance deliver a final report on incident to body which they informed on incident within 15 days from incident termination, which must contain the type and description of the incident, the time and duration of the incident, the consequences of the incident, triggered, actions taken to remedy the incident and, where appropriate, other relevant information.

In the event of incidents in ICT systems dealing with classified information operators of the ICT systems shall act in accordance with the regulations governing the field of classified information protection.

Provisions of paragraphs 1 and 7 of this Article shall not apply to independent ICT system operators.

The Government, at the proposal of the competent authority, shall regulate the incident notification procedure, the list, types and significance of incidents according to the threat level, handling and exchange of information on incidents between the authorities referred to in Article 5 hereof.

If the incident is of interest to the public, the Competent authority, or the authority referred to in paragraph 3 of this Article to whom the notifications of incidents are reported, may publish the information, after consulting with the operator of the ICT system of special importance where the incident occurred.

If the incident is related to the commission of criminal offenses that are prosecuted ex officio, the authority to whom the notification of incident has been reported shall notify the competent Public Prosecutor's Office or the ministry in charge of internal affairs.

If the incident concerns a significant impact on information security, which impact has threatened or may threaten defense of Republic of Serbia, the authority to whom the notification of incident is reported shall notify the Military Intelligence Agency.

If the incident concerns a significant impact on information security, which impact has threatened or may threaten national security, the authority to whom the notification of incident is reported shall notify the Security Information Agency.

In the event of threats, disturbances of destruction of an ICT system of special importance, the management and coordination of the implementation of measures and tasks in the said event shall be undertaken by the national emergency management office, in accordance with the law.

Incidents in ICT Systems of Special Importance that may have a Significant Impact on Information Security

Article 11a

An operator of an ICT system of special importance shall report the following incidents that may have a significant impact on information security:

1) incidents having a disruptive effect on the performance of tasks and provision of services, or causing significant difficulties in performance of tasks and provision of services;

2) incidents impacting a great number of users, lasting for a long time;

3) incidents having a disruptive effect on, or causing difficulties in performance of tasks and provision of services, with an impact on performance of tasks and provision of services of other operators of ICT systems of special importance or on public safety;

4) incidents having a disruptive effect, or causing difficulties in performance of tasks and provision of services and affecting a major part of the territory of the Republic of Serbia;

5) incidents leading to unauthorized access to protected data whose disclosure may jeopardize rights and interest of data subjects;

6) incidents resulting from incidents in the ICT system referred to in Article 6, paragraph 1, item 3) subitem (7) hereof, when the ICT system of special importance uses the information services of the ICT system referred to in Article 6, paragraph 1, item 3) subitem (7) hereof in its operation.

An operator of an ICT system of special importance shall report incidents that significantly increase the risk of onset of effects referred to in paragraph 1 above.

Submission of Statistical Data on Incidents

Article 11b

An operator of an ICT system of special importance shall, in addition to notifications of incidents referred to in article 11 hereof, submit to the national cert statistical data on all incidents in the ICT system in the previous year by 28 February of the current year.

The National CERT shall submit the aggregate statistical data referred to in paragraph 1 above to the competent authority and publish them on the portal of the national cert.

The type of statistical data referred to in paragraph 1 above shall be defined by the national cert.

International cooperation and early warnings about risks and incidents

Article 12

The Competent authority shall establish international cooperation in the field of the ICT system security, and in particular, it shall provide warnings about risks and incidents that meet at least one of the following conditions:

1) they grow quickly or tend to become high risks;
2) they overcome or can overcome national capacities;

3) they can have a negative impact on more than one country.

In case of an incident related to the commission of a criminal offense, following the notification from the Competent authority, the ministry responsible for internal affairs will forward the report in the official procedure, in accordance with the confirmed international agreements.

Independent ICT System Operators

Article 13

Independent ICT system operators will appoint special persons, or organizational units, for internal control of their own ICT systems.

The persons responsible for internal control of independent ICT system operators shall submit the report on the performed internal control to the manager of the independent ICT system operator.

Compliant Application of the Provisions on Independent ICT System Operators

Article 13a

On the National Bank of Serbia, as the operator of the ICT system, shall accordingly be applied the provisions of Art. 13, 15, 15A, 19, 22, 26, 27. And 28. of this Law, relating to Independent ICT System Operators.

On the National Bank of Serbia, as the operator of the ICT system, shall accordingly be applied the provisions of Art. 11 and 11a of this Law, relating to ICT system operators of special importance.

III. PREVENTION AND PROTECTION AGAINST SECURITY RISKS IN ICT SYSTEMS IN THE REPUBLIC OF SERBIA

National CERT

Article 14

The National CERT shall perform the tasks of coordinating the prevention and protection against security risks in ICT systems in the Republic of Serbia at the national level.

The Regulatory Agency for Electronic Communications and Postal Services shall be responsible for the activities of the National CERT.

Competences of the National Cert

Article 15

The National CERT shall collect and exchange information on the risks to the ICT systems security, and the events that jeopardize the ICT system security, and it shall inform, provide support, warn and advise, in this regard, the persons who manage ICT systems in the Republic of Serbia, as well as the public, and it shall in particular:

1) monitor the state of incidents at the national level,

2) provide early warnings, alerts and announcements, and inform relevant persons about risks and incidents,

3) respond to reported or otherwise detected incidents in ICT systems of special importance, as well as to reports by individuals and legal entities, by providing advice and recommendations on the basis of available information to persons affected by the incident, and undertake other necessary measures within its jurisdiction on the basis of the obtained

knowledge,

4) continuously prepare risk and incidents analyses,

5) raise awareness among citizens, business entities and public authorities about the importance of information security, the risks and protection measures, including the implementation of campaigns aimed at raising this awareness,

6) keeps records of Special CERTs,

7) submits quarterly reports on undertaken activities to the competent authority.

National CERT is authorized to process personal data that is addressed to the National CERT in accordance with the law governing the protection of personal data and other regulations.

Processing of data on the person referred to in paragraph 1, item 3) of this Article shall include the name, surname and telephone number and / or e-mail address and shall be performed for the purpose of recording the filed applications, informing the applicant of the status of the case and, if necessary, submitting the application to the competent authorities for further action, in accordance with the law.

The National CERT shall ensure the availability of its services at all times via various communication means.

The premises and information systems of the National CERT must be on safe locations.

To ensure the continuity of operation, the National CERT should:

1) be equipped with appropriate incident management systems;

2) be adequately staffed to ensure availability at all times;

3) rely on an infrastructure the continuity of which is ensured, or ensure redundant systems and backup working space.

The National CERT shall cooperate directly with the Competent authority, Special CERTs in the Republic of Serbia, similar organizations in other countries, with public and business entities, CERTs of independent ICT system operators, as well as with the CERT of public authorities.

The National CERT shall promote the adoption and use of prescribed and standardized procedures for:

1) management and remediation of risks and incidents;

2) classification of information on risks and incidents, or classification according to the level of incidents and risks.

Cooperation of CERTS in the Republic of Serbia

Article 15a

The National CERT, the CERT OF public authorities and CERTS of independent ICT system operators reflect continuous cooperation.

The CERTS referred to in paragraph 1 above shall hold joint meetings organized by the national cert at least three times a year, and where appropriate, in the event of incidents having a significant impact on information security in the Republic of Serbia.

Meetings of CERTS referred to in paragraph 1 above shall also be attended by representatives of the competent authority.

Meetings of CERTS referred to in paragraph 1 above may also be attended, when invited, by representatives of Special CERTS.

Supervision over the work of the National CERT

Article 16

The supervision over the work of the National CERT in the performance of the

activities entrusted by this law shall be performed by the Competent authority, which shall periodically, and at least once a year, check whether the National CERT has adequate resources, performs operations in accordance with Article 15 of this Law, and controls the effect of the established processes to manage the security incidents.

Special Centers for the Prevention of Security Risks in ICT Systems

Article 17

The special Center for the Prevention of Security Risks in ICT Systems (hereinafter: Special CERT) shall perform the tasks of prevention and protection against security risks in ICT systems within a certain legal person, a group of legal persons, a business area and the like.

The Special CERT is a legal person or an organizational unit within a legal person, which is entered in the records of special CERTs managed by the National CERT.

Entry into the records of special CERTs shall be done based on the application of a legal person the special CERT belongs to.

The records of special CERTs shall contain personal information about responsible persons, such as: name, surname, function and contact information such as address, telephone number and e-mail address.

Detailed requirements for entry into the records referred to in paragraph 3 of this Article shall be adopted by the National CERT.

Centre for Security of ICT Systems within authorities (CERT of public authorities)

Article 18

The CERT of public authorities shall perform the tasks related to the protection against incidents in the ICT systems of authorities, except for the ICT system of independent operators.

The work of the CERT of public authorities shall be carried out by the authority responsible for the design, development, construction, maintenance and improvement of the computer network of republic authorities.

The work of the CERT of public authorities shall include:

1) protection of the ICT system of the Computer network of republic authorities (hereinafter: CNRA);

2) coordination and cooperation with ICT system operators connected by CNRA in incident prevention, detection of incidents, gathering of information on incidents, and eliminating the consequences of incidents;

3) publication of professional recommendations for the protection of the ICT systems of public authorities, except the ICT system dealing with classified information.

CERT of an Independent ICT System Operator

Article 19

Independent ICT system operators shall be required to establish their own security centers for ICT systems to manage the incidents in their own systems.

The Centers referred to in paragraph 1 of this Article shall mutually exchange information about incidents, as well as with the National CERT and with the CERT of public authorities, and, if necessary, with other organizations.

The scope of work of the Center for Security of the ICT System, as organizational unit of the independent ICT system operator, besides the activities referred to in paragraphs 1 and 2 of this Article, may include:

1) development of internal acts in the field of information security;

2) selection, testing and implementation of technical, physical and organizational measures for protection, equipment and programs;

3) selection, testing and implementation of CEMR protection measures;

4) supervision of the implementation of security procedures;

3) management and use of cryptographic products;

4) analysis of the security of the ICT system in order to assess the risks;

5) training of employees in the field of information security.

Protecting when using Information and Communication Technologies

Article 19a

A Competent Authority shall undertake preventive measures for safety and protection online, as well as public interest activities, by educating and informing citizens, especially children, parents and teachers, about advantages, risks and ways of safe use of the internet, as well as through a single contact point for providing advice and receiving complaints about safety online, and forward the complaints to competent authorities for taking further action.

An electronic communications operator providing public telephone services shall enable free of charge calls to the single contact point for providing advice and receiving complaints about safety online for all subscribers.

If the complaint indicates a criminal offence, infringement of rights, health status, welfare and/or general integrity of a person, internet addictive behavior risk, the complaint shall be referred to the competent authority for handling it in accordance with its remit.

A Competent Authority is authorized for processing data on the person seeking information and advice from the competent authority pursuant to the law and other regulations.

Processing of data on the person referred to in paragraph 4 above shall include his/her name, surname and telephone number and/or e-mail address and it shall be performed in accordance with the law governing personal data protection, for the purpose of complaints recording, informing of submitter on the complaint status, and, in case it is necessary, submitting a complaint to competent authorities for taking further action, in accordance with the law.

Personal data reffered to paragraph 5 hereby are kept in accordance with the regulations governing office management.

To ensure the continuity of operation of the single contact point for providing advice and receiving complaints about safety online, the competent authority should:

1) be equipped with appropriate complaint handling systems;

2) be adequately staffed to ensure availability in work;

3) rely on an infrastructure the continuity of which is ensured.

The Government shall regulate in more detail the implementation of measures for safety and protection online referred to in paragraphs 1 and 3 above.

IV. CRYPTOSECURITY AND PROTECTION AGAINST COMPROMISING ELECTROMAGNETIC RADIATION

Competence

Article 20

The Ministry in charge of defense shall be responsible for the information security tasks related to approval of cryptographic products, distribution of crypto materials and protection against compromised electromagnetic radiation, and the tasks and activities in

accordance with the law and regulations adopted on the basis of the law.

Activities and tasks

Article 21

In accordance with this Law, the Ministry in charge of defense shall:

1) organize and implement the scientific research in the field of cryptographic security and protection against CEMR;

2) develop, implement, verify and classify the cryptographic algorithms;

3) research, develop, verify and classify its own cryptographic products and solutions for CEMR protection;

4) verify and classify national and foreign cryptographic products and solutions for CEMR protection;

5) define procedures and criteria for the evaluation of cryptographic security solutions;

6) perform the function of a national body for approval of cryptographic products, and ensure that these products are approved in accordance with the relevant regulations;

7) perform the function of a national body for protection from CEMR;

8) check the ICT system from the aspect of crypto security and protection against CEMR;

9) perform the function of a national body for distribution of crypto material, and define the management, handling, storage, distribution and recording of crypto material in accordance with the regulations;

10) plan and coordinate the production of crypto parameters (parameters of cryptographic algorithm), the distribution of crypto material and the protection against compromising electromagnetic radiation in cooperation with independent ICT system operators;

11) establish and maintain a central register of verified and distributed crypto material;

12) establish and maintain a register of issued approvals for cryptographic products;

13) create electronic certificates for cryptographic systems based on public key infrastructure (RivPs Key 1p^{A}ga5^{A}gis^{A}ige - RK1);

14) propose the adoption of regulations in the field of crypto security and protection against CEMR, pursuant to this Law;

15) perform expert supervision related to crypto security and protection against CEMR;

16) provide expert assistance to the inspector for the information security in the field of crypto security and protection against CEMR;

17) provide services for a fee to legal and natural persons, outside the public authorities, in the field of crypto security and protection against CEMR, according to the regulation of the Government on the proposal of the Minister of Defense;

18) cooperate with national and international bodies and organizations within its competencies regulated by this Law.

The funds generated from the fee for the services referred to in paragraph 1, item 17) of this Article shall be the revenues of the budget of the Republic of Serbia.

Compromising electromagnetic radiation

Article 22

CEMR protection measures for handling classified information in ICT systems shall

be applied in accordance with the regulations governing the protection of classified information.

CEMR protection measures can be applied by the operators of ICT systems who do not have this as a legal obligation, on their own initiative.

For all technical components of the system (devices, communication channels and spaces) that are at risk of CEMR, which could lead to violation of the information security referred to in paragraph 1 of this Article, a CEMR protection check and an assessment of the risk of unauthorized access to classified information using CEMR shall be performed.

The CEMR protection check shall be carried out by the Ministry in charge of defense.

The independent ICT system operators can perform CEMR checks for their own needs.

The detailed requirements for CEMR checks, and the way of assessing the risk of data leakage through CEMR shall be regulated by the Government, at the proposal of the ministry responsible for defense.

Crypto protection measures

Article 23

Crypto protection measures for handling classified information in ICT systems shall be applied in accordance with the regulations governing the protection of classified information.

Crypto protection measures may also be applied when transmitting and storing data that are not classified as secret, in accordance with the law governing the secrecy of data, when it is necessary, on the basis of the law or other legal act, to apply technical measures to limit the access to data and to protect the integrity, authenticity and non-repudiation of data.

At the proposal of the ministry responsible for defense, the Government shall regulate the technical requirements for cryptographic algorithms, parameters, protocols and information assets in the field of crypto protection used in cryptographic products in the Republic of Serbia for the purpose of protection of secrecy, integrity, authenticity and non-repudiation of data.

Approval for a cryptographic product

Article 24

Cryptographic products used to protect the transmission and storage of data designated as secrets, in accordance with the law, must be verified and approved for use.

At the proposal of the ministry responsible for defense, the Government shall closely regulate the requirements that must be met by the cryptographic products referred to in paragraph 1 of this Article.

Issuing approval for a cryptographic product

Article 25

An approval for a cryptographic product shall be issued by the ministry in charge of defense, at the request of the ICT system operator, the manufacturer of the cryptographic product or another interested person.

The approval for a cryptographic product may refer to a single copy of a cryptographic product or to a specific cryptographic product model that is produced serially.

The approval for a cryptographic product may have a validity period.

The Ministry in charge of defense shall decide upon the request for the issuance of approval for a cryptographic product within 45 days from the date of submission of a regular request, which can be extended in case of special complexity of the check for a maximum of 60 days.

An appeal shall not be allowed against the decision referred to in paragraph 4 of this Article, but an administrative dispute may be initiated.

The Ministry in charge of defense shall keep a register of issued approvals for a cryptographic product.

The register referred to in paragraph 6 of this Article shall contain personal information on persons responsible, such as name, surname, function and contact information such as address, telephone number and e-mail address.

The Ministry in charge of defense shall publish a public list of approved cryptographic product models for all models of cryptographic products for which it was emphasized in the application for approval that the cryptographic product model should be in the public list, and if the application was submitted by the manufacturer or by the person authorized by the manufacturer of the cryptographic product concerned.

The Ministry in charge of defense may revoke a previously issued approval for a cryptographic product, or change the requirements from paragraphs 2 and 3 of this Article for reasons of new knowledge related to the technical solutions applied in the product, which affect the assessment of the level of protection provided by the product.

The Government, at the proposal of the ministry responsible for defense, shall closely regulate the content of the application for the approval of a cryptographic product, the conditions for granting the approval for a cryptographic product, the method of issuing the approval, and the content of the register of issued approvals for a cryptographic product.

General approval for the use of a cryptographic product

Article 26

Independent ICT system operators shall have a general approval for the use of a cryptographic product.

The ICT system operator referred to in paragraph 1 of this Article shall independently assess the degree of protection provided by each individual cryptographic product it uses, in accordance with the prescribed requirements.

Registers in crypto protection

Article 27

Independent ICT system operators that have general approval for the use of a cryptographic products shall establish and maintain registers of cryptographic products, crypto materials, rules and regulations, and persons performing crypto protection jobs.

The register of persons performing crypto protection jobs shall contain the following personal information on persons performing crypto protection jobs: surname, father's name and name, date and place of birth, personal identity number, telephone, e-mail address, education, data on completed vocational training for crypto protection jobs, job name, date of beginning and end of work in crypto protection jobs.

The register of crypto materials for handling foreign classified information shall be maintained by the Office of the National Security Council and Classified Information Protection, in accordance with ratified international agreements.

The Government, at the proposal of the ministry responsible for defense, shall closely regulate keeping of the registers referred to in paragraph 1 of this Article.

V.INFORMATION SECURITY INSPECTION

Information security inspection activities

Article 28

The information security inspection shall perform inspection supervision over the implementation of this Law and the operation of the operator of the ICT systems of special importance, except the operators of independent ICT systems and ICT systems for handling classified information, in accordance with the law regulating inspection supervision.

The work of the information security inspection shall be performed by the ministry in charge of information security through an information security inspector.

Within the inspection supervision of the work of an ICT system operator, the information security inspector shall determine whether the requirements prescribed by this Law and the regulations adopted pursuant to this Law have been fulfilled.

Authorities of an information security inspector

Article 29

In the procedure of performing the inspection supervision, an information security inspector shall be authorized, in addition to ordering measures for which the inspector is authorized in the procedure of performing the inspection supervision established by law, to do the following:

1) order the removal of established irregularities and give a deadline for it;

2) prohibit the use of procedures and technical means that endanger or violate information security and give a deadline for it.

VI. PENAL PROVISIONS

Article 30

A penalty of 50,000.00 to 2,000,000.00 dinars shall be imposed for infringement to an operator of an ICT system of special importance if it:

1) fails to execute the entry in the registry within the time limit referred to in Article 6b hereof;

2) fails to adopt the Act on security of ICT systems referred to in Article 8 paragraph 1 of this Law;

3) fails to apply the protection measures determined by the Act on security of ICT systems referred to in Article 8, paragraph 2 of this Law;

4) fails to verify the compliance of implemented measures referred to in Article 8, paragraph 4 of this Law;

5) fails to submit the statistical data referred to in Article 11b hereof;

6) fails to comply with the order of the information security inspector within the given deadline referred to in Article 29, paragraph 1, item 1 of this Law.

For the infringement referred to in paragraph 1 of this Article, the responsible person of an operator of an ICT system of special importance shall also be punished with a fine ranging from 5,000.00 to 50,000.00 dinars.

Article 31

A penalty in the amount of 50,000.00 to 500,000.00 dinars shall be imposed on an operator of an ICT system of special importance for infringement if:

1) fails to inform the authorities referred to in Article 11, paragraphs 1, 3 and 7) hereof about incidents in the ICT system;

2) fails to deliver notifications on important events regarding incident and activities

from Article 11 paragraph 5 hereby;

3) fails to deliver final report from Article 11. paragraph 6 hereby.

For the infringement referred to in paragraph 1 of this Article, the responsible person of an operator of an ICT system of special importance shall also be punished with a fine ranging from 5,000.00 to 50,000.00 dinars.

Notwithstanding paragraphs 1 and 2 of this article, if financial institutions fails to notify National bank of Serbia about incidents, National bank of Serbia orders measures and penalties in accordance with the law governing financial institutions.

VII. TRANSITIONAL AND FINAL PROVISIONS

Time limits for adoption of secondary legislation

Article 32

The secondary legislation provided for in this Law shall be adopted within six months from the day of entry into force of this Law.

Article 33

The operators of ICT systems of special importance shall be obliged to adopt the Act on the security of the ICT system of special importance within 90 days from the date of entry into force of the secondary legislation referred to in Article 10 of this Law.

Entry into force

Article 34

This Law shall enter into force on the eight day following that of its publication in the "Official Gazette of the Republic of Serbia".