LAW
on Information Security

"Official Gazette of the RS", No 6 of 28 January 2016, 94 of 19 October 2017

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 stored, processed, searched or transmitted by elements covered under sub-items (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;

2) *ICT system operator* means a legal entity, a public sector body, or an organizational unit of a public sector body 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* means an internal or external circumstance or event that endangers or violates 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 sector body* means a state authority, an autonomous province's authority, a local self-government unit's authority, an organization vested with the exercise of public powers, a legal entity established by the Republic of Serbia, an autonomous province or a local self-government unit, as well as a legal entity predominantly or entirely financed from the budget;

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;

20) *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, in-house general acts, procedures, and the like.

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.

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, CERT of republic authorities and National CERT.

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 sector bodies, 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 sector bodies;

2) the processing of data that, in accordance with the law governing the protection of personal data, is considered to be particularly sensitive personal data;

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

(1) production, transmission and distribution of electricity;

(2) coal production and processing;

(3) research, production, processing, transport and distribution of oil and natural and liquid gas;

(4) trade of oil and petroleum products; railway, postal and air traffic;

(5) electronic communication;

(6) publication of an official gazette of the Republic of Serbia;

(7) management of nuclear facilities;

(8) use, management, protection and improvement of goods of general interest (water, roads, mineral resources, forests, navigable rivers, lakes, coasts, spas, wildlife, protected areas);

(9) production, trade and transport of weapons and military equipment;

(10) waste management;

(11) utility services;

(12) operations of financial institutions;

(13) health care;

(14) information society services intended for other information society service providers in order to facilitate the provision of their services.

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

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 minimization 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/or 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) information security issues 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.

Notifying the Competent authority of incidents

Article 11.

The operators of ICT systems of special importance shall be obliged to inform the Competent authority about incidents in ICT systems that can have a significant impact on information security breaches.

Notwithstanding paragraph 1 of this Article, the financial institutions shall send notifications to the National Bank of Serbia, the telecommunication operators to the regulatory body for electronic communications, and the operators of the ICT system dealing with classified information shall act in accordance with the regulations governing the field of classified information protection.

Provisions of paragraphs 1 and 2 of this Article shall not apply to independent ICT system operators.

The procedure for information submission, the list, types and significance of incidents and the notification procedure referred to in paragraph 1 of this Article shall be regulated by the Government.

If the incident is of interest to the public, the Competent authority, or the authority referred to in paragraph 2 of this Article to whom the notifications of incidents are reported, may order its publication.

If the incident is related to the commission of offenses that are prosecuted ex officio, the Competent authority or the authority referred to in paragraph 2 of this Article to whom the notification of incidents are reported, shall notify the competent Public Prosecutor's Office or the ministry in charge of internal affairs.

If the incident is related to the violation of the right to protection of personal data, the Competent authority or the authority referred to in paragraph 2 of this Article to whom the notifications of incidents are reported, and the independent ICT system operator shall also notify the Commissioner for Information of Public Importance and Personal Data Protection.

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.

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.

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

National Center for the Prevention of Security Risks in ICT Systems (National CERT)

Article 14.

National Center for the Prevention of Security Risks in ICT Systems (hereinafter: 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.

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, 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 by providing advice 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 sector bodies 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.

The records referred to in paragraph 1, item 6) of this Article, shall contain personal information on the responsible persons, namely: name, surname, function and contact details such as address, telephone number and e-mail address.

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 republic authorities.

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

1) management and remediation of risks and incidents;

2) classification of information on risks and incidents;

3) classification of severity of incidents and risks;

4) definition of data formats and models for the exchange of information on risks and incidents, and definition of the rules by which significant systems will be named.

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 Competent authority.

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

Article 18.

Centre for Security of ICT Systems within republic authorities (hereinafter: CERT of republic authorities) shall perform the tasks related to the protection against incidents in the ICT systems of republic authorities, except for the ICT system of independent operators.

The work of the CERT of republic 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 republic 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 republic authorities, except the ICT system dealing with classified information.

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 republic 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;

5) management and use of cryptographic products;
6) analysis of the security of the ICT system in order to assess the risks;
7) training of employees in the field of information security.

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^ga5^gis^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 products

Article 26.

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

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 a legal person if:

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

2) it 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;

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

4) it 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 a legal person 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 a legal person for infringement if it does not inform the Competent authority, or the authority in charge to ensure the implementation of standards in the field of classified data protection, the National Bank of Serbia or the regulatory body for electronic communications (Article 11, paragraphs 1 and 2).

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

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”.