LAW

on Information Security

I. BASIC PROVISIONS

Scope

Article 1

This Law shall govern the protection measures against security risks in information and communication systems, the responsibilities of entities in the management and use of information and communication systems and the procedures and measures to achieve a high general information security level and shall determine the authorities responsible for the implementation of protection measures, coordination between protection elements and monitoring of proper application of statutory protection measures, as well as the competences of the entities responsible for monitoring the implementation of this Law.

Definitions

Article 2

As used herein, the following terms shall have the meaning set forth below:

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

(1) *electronic communication networks and services* within meaning of the governing for electronic communications;

(2) any device or group of interconnected or related devices, one or more of which, pursuant to a programme, carry out automatic processing of data;

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

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

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

2) *operator of ICT system* means a natural person in the capacity of a registered entity, a legal entity, an authority or an organisational unit of an authority that uses the ICT system as part of its activities or tasks within its scope of competences;

3) *information security* means the ability of information and communication systems and networks to resist and/or mitigate, at a given level of confidence, any event that may compromise the availability, integrity, authenticity, non-repudiation and confidentiality of data that is stored, transmitted or processed, as well as of the services provided by, or accessible via, those ICT systems;

4) *integrity* means a property ensuring that data or information is not altered or destroyed in an unauthorised manner since it was created, transferred or stored;

5) *availability* means a property that ensures availability and usability of the ICT system when requested by authorised persons or processes, at the point when they need it;

6) *authenticity* means a property that ensures the possibility of checking and verifying that information was created or sent by the person who is claimed to have performed the action;

7) *confidentiality* means a property ensuring that the information and functions of the ICT system are available only to authorised persons;

8) *non-repudiation* means the ability to prove that a certain action took place or that a certain event occurred, so that it cannot subsequently be denied;

9) *risk* means the possibility of loss or disruption caused by an incident, expressed as a combination of the magnitude of such loss or disruption and the likelihood of the incident occurring;

10) *vulnerability* means a weakness or flaw of ICT products or ICT services that can be exploited by one or more cyber threats;

11) *risk management* means a set of systematic identification and assessment activities and risk control system establishment that enables planning, organising and directing protective measures so as to ensure that the risks remain within the statutory and acceptable frameworks;

12) *near miss* means an event in an ICT system that could have compromised the availability, authenticity, integrity, non-repudiation or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, ICT systems, but that was successfully prevented from materialising through timely intervention or protective measures;

13) *threat* means any circumstance, event or action that may endanger, disrupt or otherwise adversely affect the ICT system, the users of such system and other persons, with a clear likelihood of damage occurring in the event of failure to respond;

14) *significant threat* means a cyber threat which, based on its technical characteristics, can be assumed to have the potential to have a severe impact on the ICT system, its operator or users of the operator's services by causing considerable material or non-material damage;

15) *incident* means an event compromising the availability, integrity, authenticity, non-repudiation or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, the ICT system;

16) *malware* means software intentionally created to damage, disrupt, disable or make unauthorised access to information and communication systems and includes various types of harmful software, including viruses, trojans, worms, ransomware and spyware;

17) *centralised incident notifications receiving system* means an information system where data are entered on incidents and near misses in ICT systems of special importance which can significantly affect disruption of information security;

18) *incident response management* means any actions and procedures aiming to prevent, detect, analyse, and stop an incident, as well as other measures undertaken to respond to an incident an eliminate its consequences;

19) *information security crisis* means an event or a situation which puts at risk, interferes with, or prevents the operation of ICT systems of special importance, causing at the same time risks, threats or consequences of extremely large scale or intensity for the population, material assets or the environment that cannot be prevented or eliminated by regular actions of competent authorities and services, and the response to such an event or situation requires participation of several competent authorities, as well as the implementation of appropriate measures;

20) *ICT system protection measures* means technical, organisational, administrative and physical measures to manage ICT system security risks;

21) *classified data* means data identified and marked by a specific secrecy level in accordance with data secrecy legislation;

22) *classified data handling ICT system* means an ICT system designated to handle classified data in accordance with the law;

23) *authority* means a state authority, an autonomous province authority, a local self-government unit, an organisation and other legal entities or natural persons with delegated public powers;

24) *security service* means a security service within the meaning of the law regulating the basic elements of the security and intelligence system of the Republic of Serbia;

25) *independent ICT system operators* means the ministry in charge of defence affairs, the ministry in charge of internal affairs, the ministry in charge of foreign affairs, security services and the National Bank of Serbia;

26) Computer Emergency Response Team (hereinafter referred to as "CERT"*)* means a functional unit within an authority or a legal entity responsible for a set of tasks relating to prevention of and protection against incidents.

27) *compromising electromagnetic emanations (CEME)* means unintentional electromagnetic emanations during data transmission, processing or storage, the receipt or analysis of which may disclose the content of those data;

28) *cryptosecurity* means a component of information security that includes crypto-protection, cryptographic materials management and cryptosecurity methods development;

29) *cryptographic protection* means the application of methods, measures and procedures to transform data into a form that makes them inaccessible to unauthorised persons for a certain period of time or permanently;

30) *cryptographic product* means software or a device through which cryptosecurity is performed;

31) *cryptographic materials* means cryptographic products, data, technical documentation of cryptographic products, as well as corresponding cryptographic keys;

32) *security zone* means a space or a premise where classified data are processed and stored in accordance with data secrecy legislation, as well as a space or a room of key importance for the ICT system information security preservation;

33) *information assets* means information processed in accordance with the function and purpose of the ICT system; electronic records of device configuration and electronic communication networks; electronic records of interactions in ICT systems, access and use of ICT systems (so-called log records); programme code; technical and user documentation; electronic records of interactions in the electronic communication network (so-called network traffic); information that regulates the purpose and use of ICT systems, processes, protection measures, etc.

34) *information society service* means a service within the meaning of the law governing electronic commerce;

35) *information society service provider* means a legal entity that is a service provider within the meaning of the law governing electronic commerce;

36) Content Delivery Network (CDN) means a network of geographically distributed servers designed to ensure high availability, accessibility and fast delivery of digital content and services to internet users, on behalf of content and service providers;

37) *internet exchange point* means a network facility which enables the interconnection of more than two independent networks (autonomous systems), primarily for the purpose of

facilitating the exchange of internet traffic, which provides interconnection only for autonomous systems and which neither requires the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system nor alters or otherwise interferes with such traffic;

38) *domain name system (DNS)* means a hierarchical distributed naming system which enables the identification of internet services and resources, allowing end-user devices to use internet routing and connectivity services to reach those services and resources;

39) *DNS service provider* means an entity that provides publicly available recursive domain name resolution services for internet end-users or authoritative domain name resolution services for third-party use, with the exception of root name servers;

40) *trust service* means a service within the meaning of the law governing electronic documents, electronic identification and trust services in electronic commerce;

41) *trust service provider* means a provider within the meaning of the law governing electronic documents, electronic identification and trust services in electronic commerce;

42) *qualified trust service* means a service within the meaning of the law governing electronic documents, electronic identification and trust services in electronic commerce;

43) *qualified trust service provider* means a provider within the meaning of the law governing electronic documents, electronic identification and trust services in electronic commerce;

44*) cloud computing service* means a digital service that enables on- demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations;

45) *data centre service* means a service provided through structures or groups of structures dedicated to centralised accommodation, interconnection and operation of IT and network equipment providing data storage, processing and transmission including all facilities and infrastructures for power distribution and environmental control;

46) *scientific research organisation* means an organisation within the meaning of the law governing science and research;

47) *public electronic communications network* means a public electronic communications network within the meaning of the law governing electronic communications;

48) *electronic communications service* means a service within the meaning of the law governing electronic communications;

49) *managed service provider* means an entity that provides services related to the installation, management, operation or maintenance of ICT products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely;

50) *managed security service provider* means a managed service provider that carries out or provides assistance for activities relating to security risk management;

51) *top-level domain name registry (TLD name registry)* means an entity to which a specific top-level domain has been assigned and which is responsible for the management of that top-level domain, including the registration of domain names under the top-level domain and the technical operation of the top-level domain, encompassing the operation of its name servers, maintenance of databases and distribution of top-level domain zones through name servers, regardless of whether such activities are carried out by the entity itself or entrusted to third parties, except in cases where the top-level domain names are used by the registry exclusively for its own purposes;

52) *entity providing domain name registration services* means a domain name registrar or another entity acting on behalf of, or for the account of, a registrar;

53) *ICT product* means an element or a group of elements within an information and communication system;

54) *ICT service* means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of ICT systems;

55) *ICT process* means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;

56) *TLP (Traffic Light Protocol)* means a standard for controlled exchange of sensitive information in the field of information security, established to ensure effective cooperation and information sharing from the source to one or more recipients. The protocol provides a simple and intuitive scheme of four labels for indicating with whom potentially sensitive information may be shared;

57) *personal data* means any information relating to a natural person whose identity is determined or identifiable, directly or indirectly, in particular on the basis of an identifier such as a name or identification number, location data, identifiers in electronic communication networks, or one or more characteristics of his or her physical, physiological, genetic, mental, economic, cultural or social identity;

58) *administrator* means a person authorised and responsible for maintaining, managing and ensuring the functionality and security of ICT systems of special importance, in accordance with this Law and other applicable regulations;

59) *technical specification* means a document defining the technical requirements to be met by a product, process or service, in accordance with the law governing standardisation.

The gender-specific terms used in this Law and the regulations adopted pursuant to it, when used in the grammatical masculine gender, denote both natural female and male genders of the persons to whom they pertain.

Information Security Principles

Article 3

Planning and application of ICT system protection measures shall be guided by the following principles:

1) Risk management principle – the selection and the level of application of measures shall be based on risk assessment, the need to prevent risk and eliminate consequences of the risk that has occurred, including all types of emergencies;

2) Comprehensive protection principle – measures shall apply to all organisational, physical and technical and technological levels, as well as during the entire life cycle of the ICT system;

3) Expertise and good practice principle – measures shall apply in accordance with expert and scientific knowledge and experience in the field of information security;

4) Awareness and competence principle – all persons whose actions effectively or potentially affect information security should be aware of the risks and possess appropriate knowledge and skills;

5) Continual improvement principle – information security protection measures and management shall be regularly reviewed and improved to ensure their efficiency and adjustability to new threats and technological changes;

6) Equality and non-discrimination principle – ICT system protection measures shall be implemented in a manner that ensures equal treatment of all users, without discrimination on any grounds, in accordance with the law;

Personal Data Processing

Article 4

When personal data are processed within the exercise of powers and compliance with duties under this Law, such processing shall be subject to the provisions of this Law, the provisions of special laws governing specific areas, as well as the provisions of the law governing personal data protection.

II. SECURITY OF ICT SYSTEMS OF SPECIAL IMPORTANCE

ICT Systems of Special Importance

Article 5

ICT systems of special importance shall mean ICT systems which are essential for maintaining critical social and economic activities, where their interruption or disruption in the provision of services would have a significant impact on public safety, public health, the functioning of other sectors, or would create a significant systemic risk.

ICT systems of special importance shall include:

1) Essential (priority) ICT systems;

2) Important ICT systems.

Operators of essential ICT systems shall include the following:

1) Legal entities and natural persons, in the capacity of a registered entities, performing activities in the following fields:

(1) Energy and mining

- Electricity generation, except generation by customers/producers within the meaning of the law governing the use of renewable energy sources and the law governing energy;
- Combined generation of electricity and thermal energy;
- Electricity supply;
- Transmission and electricity transmission system management;

- Distribution of electricity and electricitydistribution system management, as well asdistribution of electricity and management of a closed electricity distribution system;
- Electricity storage, except storage by customers/producers within the meaning of the law governing the use of renewable energy sources;
- Organised electricity market management;
- Thermal energy generation, distribution and supply;
- Transport of oil through oil pipelines, transport of oil derivatives through product pipelines, and transport od oil and oil derivatives by other means of transport;
- Oil and natural gas exploration and production;
- Oil derivatives production;
- Oil and oil derivatives storage;
- Transport od natural gas and management of the natural gas transmission system;
- Natural gas storage and storage management;
- Natural gas distribution and distribution system management;
- Natural gas supply and public supply;
- Coal production and processing;
- Production and processing of copper, gold, lead, zinc, lithium and boron;
- Production, storage and transmission of hydrogen.

(2) Transport
- Air transport with a valid operating licence;
- Airport management;
- Air traffic control services;
- Public railway infrastructure management;
- Railway undertakings activities;
- Carriage of passengers and goods by inland waterways;;
- Port management;
- Operators vessel traffic services (VTS);
- River information services (RIS);
- Management of road infrastructure;
- Management od intelligent transport systems (ITS).

(3) Banking and financial markets
- Activities of financial institutions under the supervision of the National Bank of Serbia or the Securities Commission;
- Keeping of a register containing data on the obligations of natural and legal persons towards financial institutions;;
- Management or performance of activities relating to the functioning of the regulated market;
- Clearing and settlement of financial instruments, within the meaning of the law governing the capital market;;
- Activities of service providers related to digital assets, within the meaning of the law governing digital assets.

(4) Health care
- Health care provision;
- Work of national reference laboratories;
- Research and development of medicinal products;

- Manufacturing of pharmaceutical medicines and preparations intended for medical use;;
- Manufacturing of medicinal products Manufacturing of pharmaceutical medicines and preparations intended for medical use;
- Processing of genetic, biomedical and other data relevant for research and development in the fields of biotechnology, bioinformatics, bioeconomy, genetics and medicine.

(5) Drinking water

- Supply and distribution of water intended for human consumption, excluding distributors for which these tasks are a non-essential part of their general activity.

(6) Wastewater

- Collecting, drainage or treatment of municipal, domestic or industrial wastewater, excluding entities for which these activities do not constitute a predominant part of their business..

(7) Digital infrastructure

- Cloud computing service provision;
- Provision of data storage and hosting centre services. .

(8) ICT service management provided to operators of essential ICT systems

- Managed service provision;
- Managed security service provision;

(9) Other fields

- Nuclear facilities management;
- Provision of trust services, including qualified trust services, provision of domain name system (DNS) services, top-level domain name registry management and domain name registration services, excluding root name server operators;
- Content Delivery Network (CDN) service provision;
- Electronic communications activities;
- Provision of internet exchange point services;
- Publication the *Official Gazette of the Republic of Serbia* and keeping the Legal Information System of the Republic of Serbia;
- Fields where there is only one service provider in the Republic of Serbia and which is necessary to perform critical social and economic activities;

2) Authorities;

3) Entities designated as critical infrastructure operators in accordance with the regulations governing critical infrastructure.

In addition to the entities referred to in paragraph 3 of this Article, operators of priority ICT systems may also be designated among entities where the interruption or disruption of the operation of ICT systems:

1) may have a significant impact on public safety, national security or public health;

2) may cause a significant systemic risk, in particular in sectors where disruption may have a cross-border impact.

The entities referred to in paragraph 4 of this Article shall be designated by the ministry in charge of information security, upon obtainingthe opinion of the authority competent for the field in which the entity performs its activities.

For operators of essential ICT systems of special importance performing activities in the banking and financial markets sector referred to in paragraph 3, item 1), subitem (3), indents one, two and five of this Article, special sector-specific regulations shall apply which further or differently regulate certain matters covered by this Law, provided that such regulations ensure at least the same level of effectiveness of security risk management measures as those referred to in Article 10 of this Law, and ensure the reporting of incidents representing an information security crisis in accordance with this Law.

The National Bank of Serbia, as the competent supervisory authority for the operations of operators of essential ICT systems performing activities in the banking and financial markets sector referred to in paragraph 3, item 1), subitem (3), indents one, two and five of this Article (entities under the supervision of the National Bank of Serbia), shall, in accordance with this Law and the provisions of special laws governing the operations of such entities, adopt regulations governing information-security matters for those entities, including, inter alia, measures for the protection of ICT systems, adoption of risk-assessment acts and ICT-system-security acts, classification of incidents, submission of incident notifications, procedures relating to incident handling, reporting during and after incidents, submission of statistical data on incidents and other matters relevant to the information-system security of those entities, as well as supervision performed over them.

Operators of Important ICT systems

Article 6

Operators of important ICT systems shall include the following:

1) Legal entities and natural persons in the capacity of a registered entity performing activities in the following fields:

- Postal services within the meaning of the law governing postal services;
- Waste management within the meaning of the law governing waste management, excluding economic operators for which these activities do not constitute a predominant part of their business;
- Packaging waste management, within the meaning of the law governing packaging waste management;
- Chemicals manufacture and supply, in accordance with the law governing chemicals;
- Food production, processing and distribution in the segment of wholesale distribution and industrial production and processing;
- Manufacture of computer, electronic and optical products;
- Manufacture of electrical equipment;
- Manufacture of machinery and equipment;
- Manufacture of motor vehicles, trailers and semi- trailers and other transport equipment;

- Manufacture of medical devices and manufacture of *in vitro* diagnostic medical devices;
- Information society services within the meaning of the law on electronic commerce;
- Manufacture, trade in and transport of weapons and military equipment;
- Space services relying on ground-based infrastructure, in particular activities of management of control centres, monitoring and communication facilities, and provision of launching services.

2) Research and development institutions;

3) Legal entities and natural persons in the capacity of registered entities and the authorities referred to in Article 5 of this Law, not designated as operators of essential ICT systems according to the criteria for classification of operators.

In addition to the entities referred to in paragraph 1 of this Article, operators of important ICT systems may also be designated among entities where the interruption or disruption of the operation of ICT systems:

1) may have a significant impact on public safety, national security or public health;

2) may cause a significant systemic risk, in particular in sectors where disruption may have a cross-border impact.

The entities referred to in paragraph 2 of this Article shall be designated by the ministry in charge of information security, following the opinion of the authority competent for the field in which the entity performs its activities.

Secondary legislation setting out in detail the requirements and general and sectoral criteria, including the criteria relating to the size of economic operators, for the classification of operators of essential and important ICT systems shall be adopted by the Government, acting on proposal from the ministry in charge of information security affairs.

Ministries responsible for the fields in whichoperators of essential and important ICT systems perform their activities, and the National Bank of Serbia, shall, submit to the ministry in charge of information security proposals of sectoral criteria to classify operators of ICT systems of special importance when drafting the secondary legislation referred to in paragraph 4 of this Article.

Obligations of Operators of ICT Systems of Special Importance

Article 7

In accordance with this Law, operators of ICT systems of special importance shall:

1) File an application to be registered with the records of ICT systems of special importance;

2) Undertake appropriate technical, operational, organisational and physical measures to protect ICT systems of special importance, manage risks and prevent and mitigate the harmful consequences of incidents;

3) Carry out a risk assessment and adopt a risk assessment act;

4) Adoptan act on the security of ICT systems of special importance;

5) Check the compliance of ICT system protection measures applied under the ICT system security act at least once a year;

6) 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;

7) Submit notifications, without delay, on any incident that significantly threatened the security of the ICT system of special importance;

8) Report near-miss incidents that represent a serious threat, in accordance with this Law;

9) Submit statistical data on incidents and near misses in ICT systems.

Obligations of Independent Operators

Article 8

Independent operators shall:

1) File an application to be registered with the records of ICT systems of special importance;

2) Undertake appropriate technical, operational, organisational and physical measures to protect ICT systems of special importance, manage risks and prevent and mitigate the harmful consequences of incidents;

3) Adopt an act on the security of ICT systems of special importance;

4) Check the compliance of ICT system protection measures applied under the ICT system security act in accordance with their own rules on checking compliance of protection measures, and in any case 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) Form their own CERT to manage incidents in their systems.

Independent operators can exchange information on incidents with the Office for Information Security and, if necessary, with other organisations.

Independent operators shall not be subject to the provisions of this Law relating to reporting incidents that significantly threaten information security, the provisions on submitting statistical data on incidents and the provisions on proactive scanning of the network of operators of ICT systems of special importance.

Independent operators may, independently or in coordination with the Office for Information Security, proactively scan their own ICT systems connected to the e-Government Single Information and Communication Network to detect vulnerabilities.

Independent ICT system operators shall designate special persons or organisational units responsible for internal control of their own ICT systems.

Persons responsible for internal control within independent ICT system operators shall submit reports on performed internal controls to managers of independent ICT system operators.

Register of Operators of ICT Systems of Special Importance

Article 9

The ministry in charge of information security (hereinafter referred to as the "Ministry") shall establish and keep records of essential and important ICT systems (hereinafter referred to as the "Register") containing the following:

1) Name, registration number and head office of the operator of an ICT system of special importance;

2) Name and surname, official email address and official contact phone number of the administrator in charge of maintaining and managing the ICT system of special importance;

3) Name and surname, official email address and official contact phone number of the person responsible for the ICT system of special importance;

4) Information on the type of the ICT system of special importance, i.e. whether the ICT system of special importance is classified as essential or important;

5) Information on the field of activity of the operator of an ICT system of special importance;

6) IP address range belonging to the ICT system of special importance, which includes data on public static IP addresses;

7) Websites of the operator of ICT system of special importance;

8) Number of locations where the ICT system of special importance is situated.

In addition to the data referred to in paragraph 1 of this Article, the records may also contain supplementary data on the ICT system of special importance.

Independent ICT system operators shall be exempt from the obligation to submit the data referred to in paragraph 1 items 4), 5), 6) and 8) of this Article.

Secondary legislation setting out in detail the content and structure of the Register, as well as the manner of submitting applications for entering and changing data in the Register, shall be adopted by the Ministry.

The operator of the ICT system of special importance shall submit the data referred to paragraphs 1 and 2 of this Article to the Ministry within 90 days of the date of adoption of the secondary legislation referred to in paragraph 4 of this Article at the latest, or 90 days of the date of establishment of the ICT system of special importance at the latest.

In the event of any change in the data referred to in paragraph 1 of this Article, the operator of ICT system of special importance shall notify the Ministry of such change within 15 days of the date when such change occurred.

The data referred to in paragraph 1 items 2) and 3) shall be processed to comply with the provisions of this Law in terms of submission of notifications and warnings significant for the security of the ICT system of special importance, and to establish communication and cooperation aimed at eliminating the harmful effects of incidents and undertaking preventive actions.

The data referred to in paragraph 1, items 2) and 3) shall be processed in accordance with the law governing personal data protection and shall be stored until the purpose of processing ceases to exist, or until the data are changedin accordance with paragraph 6 of this Article.

The Ministry shall make the Register available to the Office for Information Security to comply with the provisions of this Law relating to collection and exchange of data on threats, vulnerabilities and incidents and to provide support, warnings and advice to the persons managing ICT systems.

The Register shall constitute classified data within the meaning of the law governing data secrecy.

Protection Measures for ICT Systems of Special Importance

Article 10

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

ICT system protection measures shall ensure the prevention of incidents, i.e. the prevention and mitigation of damage from incidents that compromise the exercise of competences and the performance of activities, in particular those performed when providing services to other persons.

The protection measures shall apply to all ICT systems of the operator referred to in paragraph 1 of this Article.

ICT system protection measures shall include the following:

1) Establishment of an organisational structure, with determined tasks, knowledge, competences, experience and responsibilities of employees, which is used to manage information security within the ICT system operator;
2) Collection of information on threats to information security of ICT systems;
3) Achieving the security of remote work and the use of mobile devices;
4) Ensuring that persons who use the ICT system, or manage the ICT system, are qualified for the work they perform and understand their responsibility, i.e. to ensure organisation of basic and, if necessary, advanced IT trainings for all employees and hired persons who have access to ICT systems, trainings for managers and governing bodies of ICT system operators of special importance, as well as specialised vocational trainings for employees responsible for information security management in order to provide continual education;
5) Ensuring sufficient resources for proper information security management;
6) Protection against risks arising from job changes or employment termination of persons employed by ICT system operators;
7) Identification of information assets and determination of the responsibility for their protection;
8) Classification of data so that the level of their protection corresponds to importance of the data in accordance with the risk management principle referred to in Article 3 of this Law;
9) Data medium protection;
10) Restriction of access to data and means of data processing;
11) Granting authorised access and preventing unauthorised access to the ICT system and services provided by the ICT system;
12) Determining the user's responsibility for the protection of their own means of authentication;
13) Applying the use of encryption controls and other data concealment techniques to protect the confidentiality, authenticity and integrity of data;
14) Application of protection measures to prevent unauthorised data leakage;
15) Physical protection of facilities, premises, rooms or zones where ICT system assets and documents are located and data are processed in the ICT system;
16) Protection against loss, damage, theft or other forms of compromising the security of assets that constitute the ICT system;
17) Ensuring the the proper and secureoperation of data processing facilities;
18) Application of appropriate procedures and protection measures when using cloud computing services;

19) Monitoring ICT systems in order to detect vulnerabilities and threats;
20) Restriction of access to websites that can potentially compromise the security of the ICT system;
21) Data protection and data processing resources against malicious software;
22) Data loss protection through regular creation of backup copies of data, software and systems by means of appropriate data exchange tools;
23) Storing data of events that may be important for the security of the ICT system;
24) Ensuring the integrity of software and operating systems;
25) Protection against exploitation of technical security weaknesses of the ICT system;
26) Ensuring the protection of the ICT system when performing audit testing;
27) Data protection in communication networks, including devices and lines;
28) Security of data transmitted within the ICT system operator, as well as between the ICT system operator and persons outside the ICT system operator;
29) Fulfilment of information security requirements for the management of all lifecycle stages of the ICT system, or parts of the system;
30) Protection of data used for the purposes of testing the ICT system, or parts of the system;
31) Procedures for storage and deletion of information in ICT systems, in accordance with the applicable regulations;
32) Protection of ICT system operator assets available to service providers;
33) Maintenance of the agreed level of information security and provided services in accordance with the requirements agreed with the service provider;
34) Prevention of and response to security incidents, which implies adequate exchange of information on security weaknesses of ICT systems, incidents and threats, as well as the implementation of measures to mitigate the consequences of the incident;
35) Measures that ensure the continuity of operation in emergencies that are defined in the Business Continuity Plan
36) Adoption of documents defining procedures for verifying the adequacy of protection measures;
37) Use of multifactor authentication or continuous authentication solutions, protected voice, video and text communications, and secure communication systems in emergencies within the ICT system operator.

Secondary legislation specifyingin detail theprotection measures for essential and important ICT systems, taking into accountthe principles referred to in Article 3 of this Law, national and international standards and standards applicable to relevant fields of work and relevant technical specifications, shall be adopted by the Government, acting on proposal from the Ministry.

Risk Assessment Act for ICT Systems of Special Importance

Article 11

The operator of the ICT system of special importance shall adopta risk assessment act (hereinafter referred to as the “Risk Assessment Act”) for the ICT systems it manages.

Under the Risk Assessment Act, a risk assessment shall be carried out for the ICT system of special importance, considering the degree of risk exposure, the operator size and the incident occurrence probability and its severity, as well as its potential social and economic impact.

The Risk Assessment Act shall be reviewed at least once a year.

The Risk Assessment Act shall be developed in accordance with the general risk assessment methodology for essential and important ICT systems adopted by the authority or the organisation where National CERT activities are performed.

The operator of the ICT system of special importance shall not have the duty to adopt the act referred to in paragraph 1 of this Article if it has a defined risk assessment, in other internal acts in place, which includes the general methodology requirements referred to in paragraph 4 of this Article.

Security Act for ICT Systems of Special Importance

Article 12

The operator of an ICT system of special importance shall adopt a security act for the ICT system (hereinafter referred to as the "Security Act").

The Security Act shall set out the protection measures, in particular the principles, methods and procedures for achieving and maintainingan adequate level of system security, as well as the powers and responsibilities related to the security and resources of ICT systems of special importance.

The Security Act for the ICT system of special importance shall be based on the Risk Assessment Act referred to in Article 11 of this Law. The application of ICT system protection measures shall be in accordance with the assessed risks to ensure adequate protection of the system and minimise the impact of potential incidents.

The Security Act shall be harmonised with changes in the environment and in the ICT system itself.

The operator of an essential ICT system shall, independently or by hiring external experts, check the compliance of applied measures of the ICT system with the Security Act at least once a year and shall prepare a report thereof.

The operator of an important ICT system of special importance shall, independently or by hiring external experts, carry out the check referred to in the previous paragraph at least once a year and shall prepare a report thereof.

Secondary legislation setting out in detail the content of the Security Act, the method of checking the ICT system of special importance and the content of check reports, as well as the submission of such reports to the competent authority, shall be adopted by the Government, acting on proposal of the Ministry.

Mandatory Notifications of Incidents that Significantly Compromise Information Security

Article 13

Operators of ICT systems of special importance shall submit notifications on incidents that may have a significant impact on disruption of information security without delay, but not later than 24 hours of learning about the incident.

Incidents that may have a significant impact in terms of compromising information security shall include the following:

1) Incidents that lead to the continuity interruption in operation and the provision of services, or significant difficulties in operation and the provision of services;

2) Incidents that affect a large number of service users, or last for a long period of time;

3) Incidents that lead to continuity interruption, or difficulties in the operation and provision of services, which affect the operation and the services performance of other ICT system of special importance operators or affect public safety;

4) Incidents that lead to continuity interruption, or difficulties in operation and provision of services and have an impact on a large part of the territory of the Republic of Serbia;

5) Incidents that lead to unauthorised access to protected data, the disclosure of which may threaten the rights and interests of data subjects;

6) Incidents that occurred as a result of an incident in the ICT system of the operators of essential ICT systems of special importance that perform activities in the field of digital infrastructure referred to in Article 5 paragraph 3 item 1) sub-item (7) of this Law, when the ICT system of special importance uses digital infrastructure information services in its operation;

7) Incidents that cause or may cause significant material or intangible damage to the operator of ICT system of special importance and to other natural persons and legal entities.

Operators of ICT systems of special importance shall also report near misses that constitute a serious threat and that would lead to a significant increase in the risk of the consequences referred to in paragraph 2 of this Article.

In the case of incidents in the ICT systems that handle classified data, the operators of such ICT systems shall act in accordance with the regulations governing the field of classified data protection.

Submission of Incident Notifications

Article 14

Operators of ICT systems of special importance shall submit incident notifications to the single incident notification system via the official website of the Ministry or the Office for Information Security.

Operators of essential ICT systems that perform activities in the field of banking and financial markets referred to in Article 5 paragraph 3 item 1) sub-item (3),of this Law shall submit incident notifications to the National Bank of Serbia, and if they are operators of essential ICT systems in the field of financial markets under the supervision of the Securities Commission, they shall also submit notifications to the Securities Commission.

Operators of essential ICT systems ce that perform electronic communications activities referred to in Article 5 paragraph 3 item 1) sub-item (9), indent four of this Law, and operators of important ICT systems of special importance that perform postal service activities referred to in Article 6 paragraph 2 item 1) indent one of this Law, shall submit incident notifications to the regulatory body for electronic communications and postal services.

The National Bank of Serbia and the regulatory body for electronic communications and postal services and the Securities Commission shall forward the received notifications referred to in paragraphs 2 and 3 of this Article to the single incident notification system.

Operators of ICT systems of special importance, except ICT system operators referred to in paragraphs 2 and 3 of this Article, shall notify the users to whom they provide services on incidents without delay, in the event of an incident that may cause or causes a harmful impact on the provision and use of services, as well as measures that users can undertake and use in order to mitigate or eliminate the harmful consequences of the incident.

The operators of ICT systems of special importance referred to in paragraphs 2 and 3 of this Article shall notify their users on incidents in accordance with special regulations.

An authority that received an incident notification in accordance with this Law, in case of an ICT system of special importance designated as critical infrastructure in accordance with the law regulating critical infrastructure, shall forward the information thereof to the ministries responsible for critical infrastructure sectors.

The authorities referred to in paragraphs 1–3 of this Article, which received an incident notification, shall, in the event of an incident that occurred in the ICT system of an operator of critical infrastructure determined in accordance with the law governing critical infrastructure, forward the received information without delay to the competent ministries for critical infrastructure sectors, in accordance with the regulations on classified data protection.

Content of Incident Notification

Article 15

Incident notificationshall contain the following data:

1) Information on the person submitting the notification;

2) Type and description of the incident and assessment of whether the incident is the result of a criminal offence;

3) Date and time of the beginning of the incident, or the moment of becoming aware ofthe incident, and the duration of the incident;

4) Consequences caused by the incident;

5) Activities undertaken to mitigate the consequences of the incident;

6) Initial assessment of the level of severity and impact of the incident on the ICT system of special importance, as well as indicators of compromise;

7) Information on a possible cross-border impact of the incident;

8) Data on previously reported similar incidents, if any, including the time and nature of such incidents, as well as the measures taken in those cases;

9) Other relevant information, where necessary.

Significance of Incidents according to Level of Severity

Article 16

Incidents in ICT systems of special importance that may have a significant impact on the violation of information security shall be classified as follows according to the level of severity, taking into account the consequences of the incident:

1) Low;
2) Medium;
3) High;
4) Very high.

Secondary legislation setting out in detail the incident notification procedure, the notification forms, the list of incidents by types and classification of incidents according to the level of severity shall be adopted by the Government, acting on proposal from the Ministry.

Operational Incident Response Team

Article 17

To ensure coordinated response to high and very high level incidents, the Office for Information Security shall form a permanent operational response team.

The Office for Information Security shall establish the criteria for appointment of operational response team members, as well as the performance of duties and tasks of the permanent operational response team.

Depending on the nature and consequences of the incident, the Office for Information Security may require inclusion of other authorities in the work of the operational response team within their scope of competences.

Where necessary, meetings of the operational response team can be attended by representatives of independent operators, persons involved in the work of the Coordination Body for Information Security Affairs, as well as representatives of special CERTs.

Persons participating in the work of the permanent operational response team shall be required to be certified for handling classified data.

High-Level Incident and Information Security Crisis Response Plan

Article 18

The Government shall adopt the High-Level Incident and Information Security Crisis Response Plan, acting on the proposal from the Office.

The Plan referred to in paragraph 1 of this Article shall include the following:

1) Objectives of measures and activities for response in case of high-level incidents and information security crises;
2) Acting of competent authorities in order to implement the plan;
3) Description of procedures in case of high-level incidents and information security crises;
4) Activities to improve the ability to respond to incidents, primarily plans for appropriate practice and trainings;
5) Models of cooperation with the private, non-governmental and academic sectors;
6) Mutual cooperation between competent authorities.

When preparing the Plan referred to in paragraph 1 of this Article, cooperation shall be established with authorities and legal entities the competences or tasks and activities of which are related to the planned activities.

The Plan referred to in paragraph 1 of this Article shall be periodically amended and supplemented in accordance with needs and new circumstances, and shall be fully redeveloped and readopted every three years, or earlier if circumstances changed to a significant extent.

Procedure upon Receipt of Incident Notification

Article 19

Upon receiving an incident notification in the ICT system of special importance, the Office for Information Security shall act in accordance with its competences established by law,and shall collect, analyse and exchange information on the risks to the security of the ICT system, on risks to the security of the ICT system and on the incident itself, and in this regard shall inform, provide support, warn and advise the operators of ICT systems of special importance and shall perform other tasks within its scope of competences.

After conducting an analysis, the Office for Information Security shall determine the severity level of the incident.

When the public has to be made aware of the incident or when the incident is such that it is of interest to the public, the Office for Information Security can publish information on the incident, after consultation with the operator of the ICT system of special importance where the incident occurred.

Notwithstanding paragraph 3 of this Article, the Office for Information Security may publish information on the incident which occurred at an operator of the essential ICT system that performs activities in the field of banking and financial markets referred to in Article 5 paragraph 2 item 1) subitem (3) indents one, two and five of this Law, after obtaining consent from the National Bank of Serbia or the Securities Commission.

The Office for Information Security, the National Bank of Serbia, the Securities Commission and the regulatory body for electronic communications and postal services shall forward notifications on incidents to:

1) The competent public prosecutor's office, or the ministry in charge of internal affairs, in case the incident is related to committing of criminal offences that are prosecuted *ex officio*,

2) The authority responsible for defence and counterintelligence affairs of relevance for defence of the Republic of Serbia or the authority responsible for national security affairs, in case the incident is related to a significant violation of information security that has or may have the effect of compromising national defence or national security of the Republic of Serbia.

When managing the response to incidents, the Office for Information Security, the National Bank of Serbia, the Securities Commission and the regulatory body for electronic communications and postal services shall label incident notifications or information on the incident in accordance with regulations and the Traffic Light Protocol (TLP).

Procedure for "Low" Severity Level Incidents

Article 20

In the case of incidents classified as "low" severity level incidents, the Office for Information Security shall, where necessary, provide recommendations for action to the operator of the ICT system of special importance.

Procedure for “Medium” Severity Level Incidents

Article 21

In the case of incidents classified as “medium” severity level incidents, the Office for Information Security shall provide recommendations for action to the operator of the ICT system of special importance.

Procedure for “High” Severity Level Incidents

Article 22

In the case of incidents classified as “high” severity level incidents, the Office for Information Security shall inform the Ministry thereof.

The Office for Information Security shall, in cooperation with the operational response team, prepare recommendations and measures to address the incident.

Upon receipt of the notification referred to in paragraph 1 of this Article, the Ministry shall convene a session of the Coordinating Body for Information Security Affairs.

After the incident has ended, the Office for Information Security shall prepare a final report in cooperation with the operational response team, which it shall submit to the Ministry within 30 days of the date when the incident ceases.

Procedure for “Very High” Severity Level Incidents

Article 23

In the case of incidents classified as “very high” severity level incidents that constitute an information security crisis, the management and coordination of the measures and tasks implementation shall be undertaken by the Government.

The Office for Information Security shall prepare a proposal to declare an information security crisis in cooperation with the operational response team, in accordance with the High-Level Incident and Information Security Crisis Response Plan, which shall contain:

1) Information on the incident;
2) Information on measures undertaken;
3) Reasons for declaring an information security crisis;
4) Obligation of authorities to act in accordance with their competences;
5) Measure to address the crisis.

A proposal to declare an information security crisis shall be submitted to the Ministry, which shall convene a session of the Coordination Body for Information Security Affairs upon receipt of the proposal without delay.

The Government shall, on the proposal of the Ministry, pass a decision on the information security crisis declaration and shall put an obligation on authorities to act according to the proposed measures in accordance with their competences.

The Office for Information Security shall, in cooperation with the operational response team, coordinate addressing of an information security crisis and reports to the Ministry and the Government all activities at least once weekly.

A proposal to declare the end of an information security crisis shall be submitted to the Ministry.

A decision to declare the end of an information security crisis shall be passed by the Government on the proposal of the Ministry.

After the information security crisis has ended, the Office for Information Security shall prepare a final report which it submits to the Ministry and the Government within 30 days of the date when the information security crisis ceases.

Reporting During and After Incident

Article 24

Operators of ICT systems of special importance shall:

1) Submit reports on an incident, for the duration of the incident, with the description of measures undertaken to address the incident, to the single incident notification system, as follows:

(1) Every three days in the event of medium-level incidents;

(2) Every 24 hours in the event of high and very high level incidents;

2) Submit notifications and additional reports on important events related to the incident and the activities they undertake, acting on request from the Office for Information Security;

3) Submit a final report on the incident within 15 days of the date when the incident ceases, which shall contain the following information:

(1) The type and description of the incident,

(2) The type of threat and the cause of the incident;

(3) The time and duration of the incident,

(4) The scope and degree of impact of the incident (realised risk),and the consequences caused by the incident;

(5) Information on a possible cross-border impact of the incident,

(6) Activities undertaken to eliminate the consequences of the incident and, where necessary, other information significant for recording the incident and for statistical processing.

After the incident has ended, the Office for Information Security shall prepare recommendations and advices for the protection against potential risks, based on the analysis of the incident that occurred.

Submission of Statistical Data on Incidents

Article 25

Operators of ICT systems of special importance shall, in addition to the incident notifications referred to in Article 13 of this Law, submit to the authority or the organisation responsible for National CERT statistical data on all incidents in the ICT system, including near misses, in the previous year until 28 February of the current year at the latest.

The authority or the organisation referred to in paragraph 1 of this Article shall submit reports on statistical data to the Ministry and shall publish them on its official website.

The type, form and method of submitting statistical data referred to in paragraph 1 of this Article shall be determined by the authority or the organisation referred to in paragraph 1 of this Article.

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

Competent Authority

Article 26

The public administration authority responsible for information security shall be the ministry in charge of information security affairs.

Within its competences, the Ministry shall:

1) Prepare and propose regulations and planning documents in the field of information security in accordance with this Law;

2) Keep records of operators of ICT systems of special importance;

3) Supervise the work of the Office for Information Security;

4) Carry out inspection of the implementation of this Law and the operations of operators of ICT systems of special importance, excluding independent operators of ICT systems and ICT systems for classified data handling;

5) Establish international cooperation within its competences.

Coordinating Body for Information Security Affairs

Article 27

To ensure cooperation and coordinated performance of tasks aimed at improving information security, as well as to initiate and monitor preventive and other activities in the field of information security, the Government shall establish the Coordinating Body for Information Security Affairs (hereinafter referred to as the "Coordinating Body"), as the Government's coordinating body, which shall comprise representatives of the ministries responsible for information security, defence, internal affairs, foreign affairs, justice, representatives of the security services, the Office for Information Security, the Office for Information Technologies and eGovernment, the Office of the Council for National Security and Protection of Classified data, the authority in charge of the design, harmonisation, development and functioning of the e-Government system, the General Secretariat of the Government, the National Bank of Serbia and the Regulatory Agency for Electronic Communications and Postal Services.

In order to improve certain fields of information security, expert working groups of the Coordinating Body shall be formed, which shall include representatives of other authorities, business entities, the academic community and the non-governmental sector.

Under the decision establishing the Coordinating Body, the Government shall determine its composition, its tasks, the deadline by which it submits reports to the Government and other issues related to its work.

Office for Information Security

Article 28

The Office for Information Security (hereinafter referred to as the "Office") shall be established to perform tasks of prevention of and protection against risks and incidents in ICT systems in the Republic of Serbia, as a special organisation within the meaning of the law governing the status of public administration.

The Office has the status of a legal entity.

The work of the Office shall be managed by the Director, who shall be a person with appropriate professional qualifications and at least five years of work experience in the field of information security, appointed by the Government in accordance with the law governing the status of civil servants. The Office shall have a Deputy Director, who must be a person of appropriate expertise with at least five years of work experience in the field of information security, appointed in accordance with the regulations governing the status of civil servants and who shall have the powers in accordance with the regulations governing public administration.

Supervision of Work of the Office

Article 29

The Ministry shall supervise the work of the Office in performance of its tasks, in accordance with the law governing public administration.

Competences of the Office

Article 30

The Office shall perform the following tasks within its competences:

1) Carry out prevention of and protection against security risks at the national level in accordance with this Law (tasks of the National CERT);

2) Undertake preventative and reactive measures to protect the e-Government Single Information and Communication Network in accordance with this Law (tasks of the CERTs of public authorities);

3) Maintain cooperation at the national level in the field of information security;

4) Perform the tasks of a single point of contact;

5) Perform certification of ICT systems, ICT products, ICT processes and ICT services, excluding systems, products, processes and services for the purpose of defence and security, and ICT systems for handling classified data

6) Prescribe minimum protection measures for authorities' ICT systems, in compliance with the principles referred to in Article 3 of this Law, the protection measures referred to in Article 10 of this Law, national and international standards, and standards applicable in relevant fields of work;

7) In cooperation with competent authorities and other entities in the public, academic, business and non-governmental sectors, participate in the development and implementation of

training and professional advancement programs for persons tasked with performing information security operations;

8) Cooperate and exchange information at the international level in the field of information security to keep abreast and ensure harmonisation with international regulations and standards;

9) Perform expert supervision of the work of operators of ICT systems of special importance;

10) Maintain a database of ICT products and ICT service vulnerabilities;

11) Report quarterly to the Ministry of the activities undertaken;

12) Perform other tasks in accordance with this Law.

Secondary legislation laying down in detail the manner of performing certification of ICT systems, ICT products, ICT processes and ICT services referred to in paragraph 1 item 5) of this Article shall be adopted by the Government, acting on the proposal from the Ministry.

Prevention of and Protection Against Security Risks at the National Level (National CERT)

Article 31

The Office shall carry out tasks of the National CERT as part of prevention from and protection against risks and incidents, including the following:

1) Collect and exchange information on threats, vulnerabilities, near misses and incidents and provision of support, provides support, warns, and advisesadvice to persons who manage ICT systems in the Republic of Serbia, as well as the public.

2) Monitor the situation regarding incidents in the Republic of Serbia;

3) Provide early warnings, alerts and announcements and inform relevant persons of threats, vulnerabilities and incidents;

4) Respond without delay to notified or otherwise detected incidents in ICT systems of special importance, as well as to notifications submitted by natural persons and legal entities, by providing advice and recommendations based on available information about incidents and taking other advice and recommendations based on the available information on incidents, and undertake other necessary measures within its jurisdiction based on information received;

5) At the request of the operator of an ICT system of special importance, provide assistance in monitoring the security status of the ICT system in real time or near real time;

6) At the request of the operator of the ICT system of special importance, perform a proactive scanning of the ICT system in order to detect vulnerabilities that can potentially significantly impact the security of the ICT system, whereby such scanning must not have a detrimental effect on the operations and activities of the operator;

7) Act as a coordinator for the purpose of coordinated vulnerability disclosure, in accordance with this Law;

8) Participate in developing and using technological tools enabling information exchange with operators of ICT systems of special importance and other cooperating entities;

9) Continuously prepare risk and incident analyses, based on the collected information;

10) Raise awareness among citizens, business entities and authorities of the importance of information security, risks and protection measures, including the implementation of campaigns aimed at such awareness raising;

11) Keep the Records of special CERTs;

12) Prepare reports on a quarterly basis on the activities undertaken;

13) Provide support in the collection and analysis of forensic data and provide dynamic risk and incident analyses in accordance with regulations;

14) Cooperate with CERTs of foreign states and, at their request, provide mutual assistance in accordance with its capacities and competences.

The Office shall promote the application and use of statutory and standardized procedures for the following:

1) Incident management;

2) Classification of information on incidents, or classification according to the severity level of incidents;

3) Crisis management;

4) Coordinated vulnerabilities disclosure.

The Office shall be authorised to process data on the person who reports the incident, it being understood that such data processing shall include the data subject's name, surname and telephone number and/or e-mail address and shall be carried out for the purpose of recording submitted applications, informing the applicant about the status of the case and, where necessary, forwarding the application to the competent authorities for further action, in accordance with the law.

The Office shall ensure continuous availability of its services through various means of communication.

The following requirements shall be complied with for tasks of the National CERT:

1) High level of communication channels availability by avoiding single interruption points and the use of several means for two-way contacting;
2) Premises of the National CERT and supporting information systems should be situated on safe locations;
3) The use of an adequate request management and directing system, particularly to facilitate efficient and effective information exchange;
4) Ensured confidentiality and reliability of is activities;
5) Appropriate human resource capacities;
6) Redundant systems and backup workspace in place to ensure the continuity of services.

Secondary legislation setting out in detail the procedure of proactive scanning of ICT systems referred to in paragraph 1 item 6) of this Article, the protective, technical and security conditions and measures to be met by the entity directly performing the scanning, as well as the procedure establishing the conditions to protect the security of systems, networks and data being accessed, and the method of reporting to the competent authority, shall be adopted by the Government, acting on the proposal of the Ministry.

Preventive and Reactive Measures to Protect e-Government Single Information and Communication Network (CERTs of Public Authorities)

Article 32

The Office shall perform the following tasks as part of preventive and reactive measures to protect the e-Government Single Information and Communication Network (hereinafter referred to as the "e-Government network"):

1) Protect the e-Government network;

2) Coordinate and cooperate with ICT system operators that are linked via the e-Government network in the prevention of incidents;

3) Actively participate in detecting incidents, collecting information on the incidents and removing the effects of incidents;

4) Proactively scan the networks of operators of ICT systems of special importance that use the network, provided that such scan is not detrimental to the operator's tasks and activities;

5) In case of a detected vulnerability:

(1) Inform ICT system operators that use the e-Government network about the vulnerability,

(2) Order the operators of ICT systems of special importance that use the network to undertake adequate protective measures to prevent, mitigate and remedy the consequences of the incident;

6) Provide expert recommendations for the protection of the authorities' ICT systems, except ICT systems handling classified data;

7) Pass an act governing the conduct of operators of ICT systems of special importance that use the network, in the event of an incident;

8) In cooperation with line authorities, assess the need for professional training of employees in operators of ICT systems of special importance that use the network;

9) Plan and organise the procedural and practical training in the field of information security for the employees in ICT systems of special importance that use the network;

10) Create proposals for the improvement of the security features of the e-Government network;

11) Prepare an analysis of the risks and incidents within the e-Government network;

12) Perform other tasks in accordance with the law to improve the information security of the e-Government network.

Secondary legislation setting out in detail the procedure of proactive scanning of ICT systems referred to in paragraph 1 item 4) of this Article, the protective, technical and security conditions and measures to be met by the entity directly performing the scanning, as well as the procedure establishing the conditions to protect the security of systems, networks and data being accessed, and the method of reporting to the competent authority, shall be adopted by the Government, acting on proposal of the Ministry.

Cooperation at the National Level

Article 33

The Office shall directly cooperate with the Ministry, the Regulatory Body for Electronic Communications and Postal Services, special CERTs in the Republic of Serbia, public and business entities and CERTs of independent ICT system operators.

CERTs may, in accordance with their competences and security protocols, independently establish cooperation with relevant actors from the public and private sector, with the obligation

to inform the Office for the purpose of coordination and exchange of information relevant to the national information security system.

The Office and CERTs of independent ICT system operators shall hold joint meetings organized by the Office at least three times a year and whenever appropriate in the event of incidents that significantly compromise information security in the Republic of Serbia.

The meetings referred to in paragraph 3 of this Article shall also be attended by representatives of the Ministry, and representatives of special CERTs, as well as other persons upon invitation.

When cooperating with the entities referred to in paragraph 1 of this Article, the Office shall ensure effective, efficient and safe exchange of information with the application of adequate procedures, including the "traffic light protocol" (TLP), and in compliance with regulations on personal data protection.

International Cooperation and Tasks of Single Point of Contact

Article 34

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

1) Grow rapidly or tend to become high-risk;

2) Exceed or may exceed the national capacities;

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

When exchanging the data referred to in paragraph 1 of this Article, the Office shall act in such a way as to ensure that the confidentiality of the data is not jeopardized, as well as that such data exchange does not affect the potential violation of the security of the ICT system. Data exchange referred to in paragraph 1 of this Article shall include transfer or processing of data necessary for assessing and responding to security risks and incidents in accordance with this Law. In case the data exchange relates to personal data, the Office shall ensure that such transfer or processing is carried out in compliance with the regulations governing personal data protection, including the rules relating to the transfer of data to other countries or international organisations.

If the incident is related to the commissionof a criminal offense that is prosecuted *ex officio*, the Office shall inform the competent public prosecutor's office thereof, which shall, on its own or through the competent ministry in charge of internal affairs, forward the report using the official procedure in accordance with ratified international agreements.

The Office shall perform the duties of the single point of contact for information security in case of cross-border security threats and incidents and shall cooperate with single points of contact of other countries.

Special Computer Emergency Response Teams in ICT Systems

Article 35

A Special Computer Emergency Response Team (hereinafter referred to as the "Special CERT") shall perform the tasks of prevention of and protection against security risks in ICT systems within a specific legal entity, group of legal entities, business area etc.

A Special CERT shall be a legal entity or an organizational unit within a legal entity based in the territory of the Republic of Serbia, which is registered in the Registry of special CERTs maintained by the authority or organisation in charge of the National CERT and published publicly.

Registration with the Registry of Special CERTs, maintained by the Office, shall be made based on the application of the legal entity within which the special CERT is located.

The Registry of special CERTs shall include personal data on responsible persons, including: name, surname, the position and contact data such as address, telephone number and e-mail, for the purpose of engaging special CERTs in case of security risks and incidents in ICT systems.

The authority or organisation referred to in paragraph 2 of this Article shall lay down the content and the method of registration and keeping of the records referred to paragraph 3 of this Article.

Vulnerability Database

Article 36

The authority or organisation in charge of the National CERT shall establish and maintain a vulnerability database of ICT products and ICT services in the Republic of Serbia and shall enable natural persons and legal entities, as well as manufacturers, suppliers and service providers in the ICT system, to report vulnerabilities in ICT products or ICT services on a voluntary basis, which can be reported anonymously.

The vulnerability database of ICT products and ICT services shall contain the following:

1) Data on vulnerabilities;

2) Data on vulnerabilities of ICT products or ICT services.

The Government, acting on the proposal of the Ministry, shall lay down the content, the vulnerability verification procedures, the procedures for managing technical vulnerabilities of ICT products and ICT services, and the method of recording and maintaining the database.

Domain Name Registration Database

Article 37

The organisation authorised to manage the top-level domain registry shall keep a list of authorised registrars for domain name registration in the Republic of Serbia.

The list referred to in paragraph 1 of this Article shall mandatorily contain the following data:

1) The name of the authorised registrar;

2) The seat and up-to-date contact details of the authorised registrar (e-mail address, official telephone number);

3) The Internet Protocol (IP) address range assigned to the authorised registrar, including data on public static IP addresses.

The authorised registrar shall be obliged to notify the organisation authorised to manage the top-level domain registry of any change in the data referred to in paragraph 2 of this Article within 15 days of the date when the change occurred.

Organisations authorised to manage the top-level domain registry and to provide DNS services shall be obliged to collect, store and maintain accurate and complete data on domain name registration in a separate database, with due care and with the application of technical, organisational and security measures for data protection, in accordance with the regulations governing personal data protection.

The database referred to in paragraph 4 of this Article shall contain at least the following data:

1) Domain name;

2) Date of domain registration;

3) Data on the registrant, namely: name and surname of the natural person, or the name of the legal entity, contact e-mail address and telephone number;

4) Contact e-mail address and telephone number of the person responsible for domain administration, where different from the registrant's data.

The organisations referred to in paragraph 4 of this Article shall be obliged to adopt and apply acts and procedures for verifying the accuracy and completeness of the data in the database. These procedures shall be publicly available.

The organisations referred to in paragraph 4 of this Article shall be obliged to ensure public availability of data which do not constitute personal data immediately after domain name registration, in accordance with the rules and conditions of registration of national internet domain names.

The organisations referred to in paragraph 4 of this Article shall be obliged to enable access to the data on domain name registration referred to in paragraph 2 of this Article that are not publicly available, based on lawful and reasoned requests of authorised persons or authorities, in accordance with competences granted by regulations governing their scope of work, and in compliance with the regulations governing personal data protection.

The response to the request referred to in paragraph 7 of this Article must be submitted without delay, and no later than within 72 hours from the receipt of the request.

The organisations referred to in paragraph 4 of this Article shall be obliged to adopt and publish policies and procedures for handling requests for disclosure of domain registration data, in accordance with this Law and the regulations on personal data protection. In accordance with this Article, the collection of domain registration data must not result in data duplication. The organisations referred to in paragraph 4 of this Article shall cooperate to avoid duplication and ensure compliance with the law.

The minister responsible for information security shall prescribe more detailed conditions for the collection, storage, verification and publication of data referred to in this Article, in line with best practices of national internet domain registries from the European Union, as well as the Internet Corporation for Assigned Names and Numbers (ICANN).

Protection of Children when Using Information and Communication Technologies

Article 38

The Ministry shall undertake preventive measures for the safety and protection of children on the Internet, as an activity of public interest, through education of and provision of information to children, parents and teachers about the advantages, risks and manners of safe use of the Internet, as well as through a single point for the provision of advice and receipt of reports regarding safety of children on the Internet, and shall forward the reports to competent authorities for further action.

Operators of electronic communications that provide publicly available telephone services shall provide all subscribers with a free call service to a single point for the provision of advice and receipt of reports regarding the safety of children on the Internet.

In the event that the a report alleges the existence of a criminal offense, a violation of the child's rights, health status, well-being and/or general integrity or a risk of developing Internet addiction, the report shall be forwarded to the competent authority for action in accordance with the established competences.

The Ministry shall be authorised to process data on any person who contacts the Ministry in accordance with the law governing personal data protection and other regulations.

The personal data processing referred to in paragraph 4 of this Article shall include the name, surname and telephone number and/or e-mail and shall be carried out for the purpose of recording the submitted reports, informing the person who filed the report about the status of the case and, where necessary, forwarding the report to the competent authorities for further handling, in accordance with the law.

The personal data referred to in paragraph 5 of this Article shall be stored within the time limits stipulated by the regulations governing office operations.

Secondary legislation setting out in detail the manner of implementation of measures for the security and protection of children on the Internet referred to in paragraphs 1 and 3 of this Article shall be adopted by the Government, acting on proposal from the Ministry.

IV. CRYPTOSECURITY AND PROTECTION AGAINST COMPROMISING ELECTROMAGNETIC EMANATIONS

Jurisdiction

Article 39

The Ministry in charge of defence shall be responsible for information security affairs related to the approval of cryptographic products which are used to protect the transmission and storage of data designated as secret, the distribution of cryptographic materials and protection against compromising electromagnetic emanations and the activities and tasks in accordance with the law and regulations adopted on the basis of the law.

Activities and Tasks

Article 40

In accordance with this Law, the ministry in charge of defence shall:

1) Organize and implement scientific and research work in the field of cryptosecurity and protection against CEME;

2) Develop, implement, verify and classify cryptographic algorithms;

3) Research, develop, verify and classify its own cryptographic products and CEME protection solutions;

4) Verify and classify domestic and foreign cryptographic products and CEME protection solutions;

5) Define procedures and criteria for evaluation of cryptosecurity solutions;

6) Exercise the function of the national authority for approval of cryptographic products and shall ensure that such products are approved in accordance with relevant regulations;

7) Exercise the function of the national authority for the protection against CEME;

8) Check ICT systems from the aspect of cryptosecurity and the protection from CEME;

9) Exercise the function of the national authority for the distribution of cryptomaterials and shall define the management, handling, storage, distribution and records of cryptomaterials in accordance with the regulations;

10) Plan and coordinate the creation of cryptoparameters (cryptographic algorithm parameters), the distribution of cryptomaterials and the protection against compromising electromagnetic emanations in cooperation with independent ICT system operators;

11) Create and maintain a central registry of verified and distributed cryptomaterial;

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

13) Create electronic certificates for cryptographic systems based on public key infrastructure (PKI);

14) Propose the adoption of regulations in the field of cryptosecurity and protection against CEME based on this Law;

15) Perform professional supervision related to cryptosecurity and protection against CEME;

16) Provide expert assistance to the holder of information security inspection supervision in the field of cryptosecurity and protection against CEME;

17) Provide services for a fee to legal entities and natural persons, outside the public authority system, in the field of cryptosecurity and protection against CEME according to the relevant regulation passed by the Government, acting on proposal from the Minister of Defence;

18) Cooperate with domestic and international authorities and organizations within the scope of competences regulated by this Law.

The proceeds of the fee charged for the provision of services referred to in paragraph 1 item 17) of this Article shall constitute revenue of the national budget of the Republic of Serbia.

Compromising Electromagnetic Emanations

Article 41

Protection measures against CEME in the ICT system for handling classified data shall be applied in accordance with the regulations governing the protection of classified data.

Protection measures against CEME can be applied on own initiative by ICT system operators who are not legally obliged to do so.

For all technical components of the system (devices, communication channels and spaces) where there is a risk of CEME, which could lead to the breach of information security referred to in paragraph 1 of this Article, a check of the protection against CEME and the risk assessment of unauthorised access to classified data via CEME shall be carried out.

The check of the protection against CEME shall be carried out by the ministry in charge of defence.

Independent ICT system operators may check CEME for their own purposes.

Secondary legislation setting out in detail the requirements to check CEME and the method of assessing the risk of data leakage through CEME shall be adopted by the Government, acting on proposal from the ministry in charge of defence.

Cryptosecurity Measures

Article 42

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

Cryptosecurity measures can also be applied when transferring and storing data that is not marked as secret in accordance with the law governing data secrecy, when, based on the law or other legal act, it is necessary to apply technical measures to limit access to data and to protect the integrity, authenticity and non-repudiation of data.

Secondary legislation setting out in detail the technical requirements for cryptographic algorithms, parameters, protocols and information assets in the field of cryptography that are used in cryptographic products in the Republic of Serbia to protect secrecy, integrity, authenticity, or non-repudiation of data shall be adopted by the Government, acting on proposal from the ministry in charge of defence.

Cryptographic Product Approval

Article 43

Cryptographic products used to protect the transmission and storage of data classified in accordance with the law shall be verified and approved for use.

Secondary legislation setting out in detail the requirements to be met by the cryptographic products referred to in paragraph 1 of this Article shall be adopted by the Government, acting on proposal from the ministry in charge of defence.

Issuance of Cryptographic Product Approvals

Article 44

Cryptographic product approvals shall be issued by the ministry in charge of defence, at the request of the ICT system operator, the manufacturer of the cryptographic product or other interested person.

Cryptographic product approvals may refer to an individual copy of the cryptographic product or to a specific model of the cryptographic product that is produced in series.

Cryptographic product approvals may have an expiration date.

The Ministry in charge of defence shall decide on the request for the issuance of a cryptographic product approval within 45 days of the date of submission of the proper request, which can be extended for maximum 60 days in case of a particularly complex check.

Appeals shall not be allowed against the decision referred to in paragraph 4 of this Article, but it can be challenged in an administrative dispute an administrative dispute can be initiated.

The Ministry in charge of defence shall maintain a register of issued cryptographic product approvals.

The register referred to in paragraph 6 of this Article shall contain personal data on responsible persons, including: name, surname, title and contact data such as address, telephone number and email. The Ministry in charge of defence shall publish a public list of approved models of cryptographic products for all models of cryptographic products for which the request for approval states that the model of the cryptographic product should be on the public list, if the request was submitted by the manufacturer or a person authorised by the manufacturer of the cryptographic product in question.

The Ministry in charge of defence may withdraw a previously issued cryptographic product approval or change the requirements referred to in paragraphs 2 and 3 of this Article due to new findings related to the technical solutions applied in the product, which affect the assessment of the degree of protection provided by the product.

Secondary legislation setting out in detail the content of requests for issuance of cryptographic product approvals, the requirements for issuing cryptographic products approvals, the method of issuing approvals and keeping of the register of issued cryptographic product approvals shall be adopted by the Government, acting on proposal from the ministry in charge of defence.

General Authorisation for the Use of Cryptographic Products

Article 45

Independent ICT system operators shall have a general authorisation to use cryptographic products.

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

Cryptosecurity Registers

Article 46

Independent ICT system operators generally authorised to use cryptographic products shall organise and maintain registers of cryptographic products, cryptomaterials, rules and regulations and persons performing cryptography tasks.

The register of persons performing cryptosecurity tasks shall contain personal data on persons performing such tasks, including: surname, father’s name and first name, date and place

of birth, personal identification number, telephone, e-mail, education, data on completed professional training for cryptography posts, job title, start and end date of appointment to cryptosecurity posts.

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

Secondary legislation setting out in detail the keeping of the registers referred to in paragraph 1 of this article shall be adopted by the Government, acting on proposal from the ministry in charge of defence.

VI. COMPETENCES AND RESPONSIBILITIES OF ENTITIES SUPERVISING THE IMPLEMENTATION OF THIS LAW

Inspectorate for Information Security

Article 47

The Inspectorate for Information Security shall supervise the implementation of this Law and the work of operators of ICT systems of special importance, except independent operators of ICT systems and ICT systems handling classified data, in accordance with the law governing inspection.

Information security inspections shall be performed by the Ministry through information security inspectors.

As part of inspection of the work of ICT system operators, information security inspectors shall determine whether the requirements laid down by this Law and the regulations adopted on the basis of this Law have been met.

Powers of Information Security Inspectors

Article 48

In addition to imposing measures which inspectors are authorised to impose when conducting inspections pursuant to the law, information security inspectors shall be authorised to:

1) Order toremedyidentified irregularities and set a reasonable timeframe for compliance;

2) Prohibit the use of procedures and technology assets that compromise or breach information security and set a timeframe for compliance;

3) Require the operator of the ICT system of special importance to perform a scanning, configuration and penetration testing of the ICT system in order to identify potential security vulnerabilities, in accordance with the risk assessment;

4) Order the inspected entity to make information on non-compliance with the provisions of this Law publicly available, when there is a justified public interest, in the manner provided for by the law;

5) Order the inspected entity to designate a person with precisely determined powers who will supervise and monitor compliance with the provisions of this Law and the ordered measures within a specified period of time.

6) Propose to the competent authority, conformity assessment body or other competent body to temporarily suspend or revoke a certificate, licence or other act confirming compliance with requirements, if the inspected entity fails to remedy the irregularities within the prescribed period;

7) Initiate proceedings under competent court or other competent authority to impose a temporary ban on the performance of managerial functions on a person who performs management tasks on behalf of the inspected entity, if such person's conduct prevents compliance with this Law and the imposed measures.

Secondary legislation further regulating the procedure of scanning, configuration and penetration testing of ICT systems for the purpose of identifying potential security vulnerabilities referred to in paragraph 1, item 3 of this Article, the protective, technical and security requirements and measures that the entity directly carrying out such activities must meet, as well as the procedure for determining conditions aimed at protecting the security of systems, networks and data accessed, and the manner of reporting to the competent authority, shall be adopted by the Government, acting on proposal from of the Ministry.

Expert Supervision

Article 49

Expert supervision of the application of this Law and the work of operators of ICT systems of special importance, except for independent operators of ICT systems and ICT systems handling classified data, shall be carried out by the Office, in accordance with the law governing inspection.

Expert supervision tasks shall be performed by the authorised person employed at the Office (hereinafter referred to as: authorised person).

In the expert supervision procedure, the authorised person shall have the duty and the right to control the following:

1) Adequacy of assessed risks, taking into account the level of risk exposure, the size of the operator and the probability of incident occurrence and its seriousness, as well as its potential social and economic impact;

2) The security level of technological procedures and technical means the ICT system operator of special importance uses to apply protection measures;

3) Proper implementation of checks aimed at verifying compliance of the measures applied in the ICT system with the security act;

4) Implementation of recommendations and measures in case of incidents that significantly endanger information security.

If, in the course of expert supervision, the Office finds irregularities, deficiencies or omissions in the application of this Law and regulations passed based on this Law, it shall notify the supervised entity thereof and shall set the timeframe for their rectification.

The time limit referred to in paragraph 4 of this Article cannot be shorter than eight days of the date of receipt of such notification, except in cases which require urgent acting.

If the Office finds that the supervised entity did not eliminate the identified irregularities, shortcomings or omissions in the application of this Law or regulations passed based on this Law within the determined deadline, it shall file a report with the inspectorate.

The Office shall, on request of the information security inspector, perform expert supervision and submit information on facts found.

The form of the identity document and the manner of issuance of the identity document shall be determined by the Office.

The identity document of the authorised person shall contain: the national coat of arms of the Republic of Serbia and the name of the Office, the name and surname of the authorised person, a photograph of the authorised person, the official number of the identity document, the date of issuance of the identity document, the official stamp of the Office, the signature of the Director of the Office, and the following printed text: "The holder of this identity document has authorisations in accordance with the provisions of Article 49 paragraphs 3 and 4 of the Law on Information Security".

VII. MISDEMEANOUR PROVISIONS

Article 50

A fine in an amount between RSD 50,000 and RSD 2,000,000shall be imposed on a legal entity that is the operator of an essential ICT system for an infringement if:

1) It fails to act in accordancewith the provisions on registration with the registar referred to in Article 9 of this Law;
2) Fails to adopt the Risk Assessment Act referred to in Article 11 paragraph 1 of this Law;

3) Fails to adopt the Security Act for ICT Systems referred to in Article 12 paragraph 1 of this Law;

4) Fails to apply the protection measures specified under the Security Act fir ICT Systems referred to in Article 12 paragraph 2 of this Law;

5) Fails to check the compliance of applied measures referred to in Article 12 paragraph 5 of this Law;

6) Fails to submit the statistical data referred to in Article 25 paragraph 1 of this Law;

7) Fails to comply with an order by the information security inspector within the specified time limit referred to in Article 47 paragraph 1 item 1) of this Law.

A fine in an amount between RSD 10,000and RSD 500,000shall be imposed on a natural person in the capacity of a registered entity that is the operator of the essential ICT system for the infringement referred to in paragraph 1 of this Article.

A fine in an amount between RSD 5,000 and RSD 50,000 shall be imposed on the responsible person of a legal entity or an authority that is the operator of the essential ICT system for the infringement referred to in paragraph 1 of this Article.

Article 51

A fine in an amount between RSD 50,000and RSD 1,000,000 shall be imposed on a legal entity that is the operator of an important ICT system for an infringement if it:

1) Fails to act in accordance with the provisions on the registration in the records referred to in Article 9 of this Law;

2) Fails to adopt the Risk Assessment Act referred to in Article 11 paragraph 1 of this Law;

3) Fails to adopt the Security Act for ICT Systems referred to in Article 12 paragraph 1 of this Law;

4) Fails to apply the protection measures specified in the Security Act for ICT Systems referred to in Article 12 paragraph 2 of this Law

5) Fails to verifythe compliance of applied referred to in Article 12 paragraph 5 of this Law;

6) Fails to submit the statistical data referred to in Article 25 paragraph 1 of this Law;

7) Fails to comply with an order by the information security inspector within the specified time limit referred to in Article 48 paragraph 1 item 1) of this Law.

A fine in an amount between RSD 10,000and RSD 250,000 shall be imposed on a natural person in the capacity of a registered entity that is the operator of the important ICT system for the misdemeanours referred to in paragraph 1 of this Article.

A fine in an amount between RSD 5,000and RSD 50,000shall be imposed on the responsible person of a legal entity or an authority that is the operator of the important ICT system ance for the infringement referred to in paragraph 1 of this Article.

Article 52

A fine in an amount between RSD 50,000 and RSD 500,000shall be imposed on a legal entity that is the operator of an essential ICT system for a misdemeanour if it:

1) Fails to inform the authorities referred to in Article 14 paragraphs 1 to 3 of this Law of the incidents in the ICT system referred to in Article 13 paragraph 2 of this Law;

2) Fails to inform the users to whom it provides services in case of an incident that may compromise or compromises the provision and use of services in accordance with Article 14 paragraph 5 of this Law;

3) Fails to submit notifications and reports during and after the incident, as referred to in Article 24 of this Law;

A fine in an amount between RSD 10,000and RSD 500,000shall be imposed on a natural person in the capacity of a registered entity that is the operator of the essential ICT system for the infringement referred to in paragraph 1 of this Article.

A fine in an amount between RSD 5,000and RSD 50,000shall be imposed on the responsible person of a legal entity or an authority that is the operator of the essential ICT system for the infringement referred to in paragraph 1 of this Article.

Notwithstanding paragraphs 1 to 3 of this Article, if an operator of an essential ICT systems of special importance referred to in Article 14, paragraph 2 of this Law fails to inform the National Bank of Serbia of incidents in the ICT system of special importance, or fails to inform its users of incidents in accordance with Article 14, paragraph 6 of this Law, the National Bank of Serbia shall

impose on such operator measures and sanctions in accordance with the law governing its operations.

Article 53

A fine in an amount between RSD 50,000and RSD 500,000 shall be imposed on a legal entity that is the operator of the important ICT system for a misdemeanour if it:

1) Fails to inform the authorities referred to in Article 14 paragraphs 1 to 3 of this Law on the incidents in the ICT system referred to in Article 13 paragraph 2 of this Law;

2) Fails to inform the users to whom it provides services in case of an incident that may compromise or compromises the provision and use of services in accordance with Article 14 paragraph 5 of this Law;

3) Fails to submit notifications and reports during and after the incident, as referred to in Article 24 of this Law.

A fine in an amount between RSD 10,000 and RSD 250,000 shall be imposed on a natural person in the capacity of a registered entity that is the operator of the essential ICT system for the misdemeanoursreferred to in paragraph 1 of this Article.

A fine in an amount between RSD 5,000 and RSD 50,000 shall be imposed on the responsible person of a legal entity or an authority that is the operator of the important ICT system for the infringement referred to in paragraph 1 of this Article.

VIII. TRANSITIONAL AND FINAL PROVISIONS

Article 54
Timeframe for Adopting Secondary Legislation

The secondary legislation provided for by this Law shall be adopted within twelve months of the date when this Law comes into force.

High-Level Incident and Information Security Crisis Response Plan referred to in Article 18 of this Law shall be adopted within eighteen months of the date when this Law comes into force.

Article 55

Until the adoption of the secondary legislation referred to in Article 6 of this Law, operators of ICT systems of special importance determined under the Law on Information Security (*Official Gazette of the Republic of Serbia* Nos. 6/16, 94/17 and 77/19) shall continue to act in accordance with the obligations established under Articles 6a to 11b of that Law until 31 December 2025.

Operators of ICT systems of special importance determined under the Law on Information Security (*Official Gazette of the Republic of Serbia* Nos. 6/16, 94/17 and 77/19) shall be subject to the penal provisions referred to in Articles 30 and 31 of that Law the date referred in Paragraph 1 of this article.

Operators of ICT systems of special importance shall adopt the act referred to in Article 11 paragraph 1 of this Law within 18 months of the date when this Law comes into force.

Authorities or organisations where tasks of the National CERT are performed shall adopt a general risk assessment methodology for ICT systems of special importance referred to in Article 11 paragraph 4 of this Law within nine months of the date when this Law comes into force.

Operators of ICT systems of special importance shall adopt the act referred to in Article 12 of this Law within 18 months of the date when this Law comes into force.

Article 56

The Office for Information Security shall be established and shall begin to perform tasks within its mandate specified under this Law on 1 January 2027.

Tasks of the Office for Information Security specified under this Law, except for the tasks of the National CERT, shall be performed by the Office for Information Technologies and e-Government in the period starting 6 months of the date when this Law comes into force until 1 January 2027.

The Regulatory Agency for Electronic Communications and Postal Services shall perform the tasks of the National CERT specified under this Law until establishment of the Office for Information Security, i.e. until 1 January 2027.

The Office for Information Security shall assume the rights, duties, employees, objects, equipment, office assets and archives from the Regulatory Agency for Electronic Communications and Postal Services created in the performance of the tasks of the National CERT which are necessary for expert tasks specified under this Law.

Starting from the date referred to in paragraph 1 of this Article, the Office for Information Security shall assume the rights, duties, employees, objects, equipment, office assets and archives from the Office for Information Technologies and e-Government created in the performance of the tasks specified under this Law within the sphere of competences of the Office for Information Security.

Article 57

Repeal of the Law on Information Security

On the date when this Law comes into force, the Law on Information Security (*Official Gazette of the Republic of Serbia* Nos. 6/16, 94/17 and 77/19) shall cease to be valid, except for the provisions of Articles 6a–11b and Articles 30 and 31, which shall remain in effect until 31 December 2025..

Secondary legislation passed based on the Law on Information Security (*Official Gazette of the Republic of Serbia* Nos. 6/16, 94/17 and 77/19) shall apply until the entry into force of the secondary legislation adopted in accordance with this Law.

Article 58
Entry into Force

This Law shall come into force on the eighth day of the date of its publication in *the Official Gazette of the Republic of Serbia*, expect Article 29 which slall apply from 1 January 2027.