DATA SECRECY LAW

("Official Gazette of the Republic of Serbia, No. 104/2009)

I BASIC PROVISIONS

Scope of Law

Article 1

This Law shall govern a single system of the classification and protection of secret data which are of interest for the national security and public safety, defence, internal and foreign affairs of the Republic of Serbia; protection of foreign classified data; access to classified data and their declassification; competence of authorities and oversight of the implementation of this Law, as well as accountability for non-implementation of obligations arising from this Law, and other issues of importance for data secrecy protection.

Terms

Article 2

For the purposes of this Law:

1) *Data of interest for the Republic of Serbia* means any data or documents in possession of a public authority, related to territorial integrity and sovereignty, protection of the constitutional order, human and minority rights and freedoms, national security and public safety, defence, internal affairs and foreign affairs;
2) *Classified data* means any data of interest for the Republic of Serbia, which have been classified and for which a level of secrecy has been determined by law, other regulations or decisions of a competent authority brought under law;
3) *Foreign classified data* means any data delivered to the Republic of Serbia by another country or an international organisation, committing the Republic of Serbia to keep them as classified data; as well as classified data arising from cooperation between the Republic of Serbia and other countries, international organisations and other international entities, under an international agreement concluded by the Republic of Serbia with another country, international organisation or other international entity;
4) *Document* means any data bearer (paper, magnetic or optical medium, disk, USB memory, smart card, compact disc, microfilm, video and audio tracks, etc.), recording or memorising classified data,
5) *Classification of data* means the procedure of classifying data as secret and determining the level and duration of secrecy;
6) *Determining the level of secrecy* means marking classified data as: "TOP SECRET", "SECRET", "CONFIDENTIAL" OR "RESTRICTED",
7) *Public authority* means a state authority, territorial autonomy, local self-government authority, an organisation vested with public powers, as well as a legal person established by

a state authority or financed wholly or predominantly from the budget, which handles classified data, i.e. creates, collects, keeps, uses, exchanges or otherwise processes classified data;

8) *Security clearance* means a procedure conducted by a competent authority prior to issuing a certificate for access to classified data, with a view to collecting information on possible security risks and obstacles to safe access to classified data;
9) *Damage* means the infringement of interests of the Republic of Serbia arising from unauthorised access to, disclosure, destruction and misuse of classified data, or from other acts related to processing classified data and foreign classified data;
10) *Classified data controller* means a natural person or an organisational unit of a public authority undertaking measures to protect classified data under the provisions of this Law (hereinafter: the controller);
11) *Data user* means any citizen of the Republic of Serbia or a legal person seated in the Republic of Serbia, to whom a certificate has been issued by a competent authority, or a foreign natural or legal person granted a security clearance for access to classified data under a concluded international agreement (hereinafter: permission), as well as a public authority official who has the right of access to and use of classified data without a certificate under this Law;
12) *Security risk* means an actual possibility of jeopardising classified data security;
13) *Protection measures* means general and special measures undertaken to prevent any damage, i.e. measures intended to ensure administrative, information and telecommunications, personal and physical security of classified data and foreign classified data.

Unclassified data

Article 3

Data marked as classified with a view to concealing crime, exceeding authority or abusing office, or with a view to concealing some other illegal act or proceedings of a public authority, shall not be considered classified.

Right of access

Article 4

Access to classified data shall be possible in the manner and under the conditions established by this Law, regulations adopted based on this Law and international agreements.

Purpose of data collection

Article 5

Classified data may be used only for the purpose for which they have been collected under law.

Data keeping and use

Article 6

Classified data shall be kept and used in accordance with the protection measures prescribed by this Law, regulations adopted based on this Law and international agreements.

Any person using classified data or any person acquainted with their contents shall be committed to keeping the data regardless of the manner in which they have learned about such classified data.

The obligation arising from paragraph 2 of this Article shall survive the termination of office or employment, or the termination of duty or membership in a public authority or relevant authority.

Protection of trade and other secrets

Article 7

The protection of trade and other secrets shall be regulated by special laws.

II DATA CLASSIFICATION

Data that can be classified

Article 8

Data that can be classified as secret shall be any data of interest for the Republic of Serbia, whose disclosure to an unauthorised person would result in damage, if the need to protect the interest of the Republic of Serbia prevails over the interest to have free access to information of public importance.

The data from paragraph 1 of this Article are particularly relevant to:

1) national security of the Republic of Serbia, public safety, or defence, foreign, security and intelligence affairs of public authorities;
2) relations between the Republic of Serbia and other countries, international organisations and other international entities;
3) systems, equipment, projects, plans and structures in connection with the data from items 1) and 2) of this paragraph;
4) scientific, research, technological, economic and financial affairs in connection with the data from items 1) and 2) of this paragraph.

Persons authorised to classify data

Article 9

Data classification shall be performed by authorised persons under the conditions and in the manner prescribed by this Law.

The authorised persons shall be:

1) the President of the National Assembly;
2) the President of the Republic;
3) the Prime Minister;
4) the head of a public authority;
5) elected, appointed or nominated public authority officials, authorised to classify data by law or regulation adopted under law, or authorised in writing by the head of a public authority;
6) persons employed by a public authority, who have been authorised in writing for data classification by the head of the public authority.

The authorised persons from paragraph 2 items 5) and 6) of this Article may not delegate their authority to other persons.

Data classification procedure

Article 10

The authorised persons from Article 9 paragraph 2 of this Law shall classify data during their creation, i.e. when the public authority begins to perform an activity resulting in the creation of classified data.

As an exception to paragraph 1 of this Article, an authorised person may also classify data subsequently, upon fulfilling the criteria established by this Law.

In classifying data, an authorised person shall assess possible damage to the interest of the Republic of Serbia.

A person employed by or performing certain tasks for a public authority shall be obliged, within his/her tasks or powers, to inform an authorised person of any data that can be classified as secret.

Decision on determining classification levels

Article 11

A decision on determining the level of classification shall be brought based on the assessment contained in Article 10 paragraph 3 of this Law, and in accordance with that decision a document shall be given a classification marking envisaged by this Law (hereinafter: the classification marking).

In determining the level of classification, an authorised person shall assign the lowest level of classification necessary to prevent harm to the interests of the Republic of Serbia.

If a document contains data that can be given different levels of classification, an authorised person shall, in relation to such levels of classification, assign the higher level of classification.

The decision set out in paragraph 1 of this Article shall be brought in writing and shall contain a rationale.

Special cases in data classification and marking

Article 12

An authorised person shall classify as secret any information developed by merging or connecting pieces of information that are not secret in their own right, if such merging and connecting result in a piece of information that should be protected for the reasons established by this Law.

A document containing data that have already been classified as secret and given different levels and duration of classification, shall be assigned, in relation to such data, the higher level of classification and the longer duration of classification of the contained information.

If a smaller part of a document contains classified data, that part shall be separated from and attached to the document as a separate enclosure marked with a level of classification.

Classification markings

Article 13

A document containing classified data shall be marked with:

1) a classification level;
2) the manner in which it is to be declassified;
3) details on the authorised person;
4) details on the public authority.

As an exception to paragraph 1 of this Article, a piece of information shall be considered classified if the document which contains it is marked only with the level of classification.

The Government shall prescribe the manner and procedure of marking the level of classification, i.e. the document.

Levels of classification and contents of data

Article 14

The data from Article 8 of this Law shall be assigned one of the following levels of classification:

1) “TOP SECRET“, which is assigned with a view to preventing irreparable grave damage to the interests of the Republic of Serbia;
2) “SECRET“, which is assigned with a view to preventing grave damage to the interests of the Republic of Serbia;
3) “CONFIDENTIAL“, which is assigned with a view to preventing damage to the interests of the Republic of Serbia;
4) “RESTRICTED“, which is assigned with a view to perventing damage to the operation or performance of tasks and activities of the public authority which defined them.

In determining the level of data classification, only the levels of classification from paragraph 1 of this Article may be applied.

The Government shall define more detailed criteria for determining the “TOP SECRET“ and “SECRET“ levels of classification, upon obtaining an opinion of the National Security Council.

The Government shall define more detailed criteria for determining the “CONFIDENTIAL“ and “RESTRICTED“ levels of classification, at the proposal of the competent minister or the head of a public authority.

Marking of foreign classified data

Article 15

A document containing foreign classified data shall keep the classification level marking which it has been assigned by the foreign country or international organisation.

In the case of documents intended for cooperation with foreign countries, international organisations or other subjects of international law, apart from the terms from Article 14 of this Law, the following markings may be used in the English language in marking the classification level of a document:

1) The “TOP SECRET“ level corersponds to the marking “STATE SECRET“ in Serbian;
2) The “SECRET“ level corresponds to the marking “STRICTLY CONFIDENTIAL“ in Serbian;
3) The “CONFIDENTIAL“ level corresponds to the marking “CONFIDENTIAL“ in Serbian;
4) The “RESTRICTED“ level corresponds to the marking “FOR INTERNAL USE“ in Serbian.

Duration of data classification

Article 16

The classification of data shall terminate:

1) on the date specified in the document containing the secret data;
2) with the occurrence of a particular event specified in the document containing the secret data;

3) with the expiry of the time period established by law;
4) with declassification;
5) if the data have been made available to the public.

An authorised person may change the established declassification method, if there are well-founded reasons for such a change in accordance with law.

An authorised person shall be bound to inform in writing the public authorities and persons that have received classified data or have access to such data, of the change from paragraph 2 of this Article.

Declassification by determining a date

Article 17

If within the classification procedure an authorised person establishes that reasons for the classification of data cease on a specific date, he/she shall determine the date of declassification and specify it in the document containing such data.

Declassification upon the occurrence of a specific event

Article 18

If within the classification procedure an authorised person establishes that reasons for the classification of data cease with the occurrence of a specific event, he/she shall determine that classification should cease with the occurrence of that event and shall specify the event in the document containing such data.

Declassification upon the expiry of a time period

Article 19

Unless the declassification of data is specified under Articles 17 and 18 of this Law, classification shall cease with the expiry of the time period established by this Law.

The legal time period of declassification from paragraph 1 of this Article shall be determined according to the level of classification as follows:

1) for data marked as “TOP SECRET” – 30 years;
2) for data marked as “SECRET” – 15 years;
3) for data marked as “CONFIDENTIAL” – 5 years;
4) for data marked as “RESTRICTED” – 2 years.

The time periods from paragraph 2 of this Article shall start running as of the date of classification.

Extension of classification time periods

Article 20

If upon the expiry of the time period from Article 19 paragraph 2 of this Law the reasons for keeping data classified continue, an authorised person may extend the time period of declassification once, at most for the period determined for the classification level involved.

Apart from the authorised person from paragraph 1 of this Article, the Government may extend the time period of classification in the following cases:

1) if the disclosure of such data would result in irreparable grave damage to the national security and particularly important state, political, economic or military interests of the Republic of Serbia;
2) if the extension is envisaged by an international agreement or other international obligations of the Republic of Serbia;
3) if the disclosure of such data would result in irreparable grave damage to the fundamental human and civil rights of one or more persons, or put in jeopardy the safety of one or more persons.

In the case described in paragraph 2 of this Article, the Government may extend the time period of declassification for the period determined for the classification level involved.

Declassification of data

Article 21

In the declassification procedure it should be established that a data is declassified before the expiry of the time period from Articles 17 to 20 of this Law.

A decision on declassification shall be brought based on the facts and circumstances because of which a data ceases to be of interest for the Republic of Serbia.

The decision from paragraph 2 of this Article shall be brought on the basis of a periodical classification assessment, declassification proposal, or a decision of the competent state authority.

Periodical classification assessment

Article 22

An authorised person shall make a periodical classification assessment on the basis of which he/she can declassify data in the following manner:

1) for data marked as “TOP SECRET”, at least once in ten years;
2) for data marked as “SECRET”, at least once in five years;

3) for data marked as “CONFIDENTIAL”, at least once in three years;
4) for data marked as “INTERNAL”, at least once a year.

If an authorised person establishes that the reasons from Article 21 paragraph 2 of this Law exist, he/she shall immediately bring a decision on declassification, which has to contain a rationale.

Data declassification proposal

Article 23

The user of secret data may propose data declassification to an authorised person.

An authorised person shall be bound to consider the proposal from paragraph 1 of this Article and to inform the proposer thereof.

Declassification within the control procedure

Article 24

In conducting the control procedure, the Office of the Council for National Security and Protection of Secret Data (hereinafter: the Council Office) may request an authorised person to make a special assessment of data classification, based on which it shall bring a declassification decision on its own.

Data declassification under a decision of the competent authority

Article 25

An authorised person of the public authority shall declassify data or documents containing secret data, and enable the petitioner, i.e. the applicant, under the decision of the Commissioner for Information of Public Importance and Personal Data Protection, in appeal procedures or based on the ruling of the competent court in proceedings upon complaint, to exercise his/her rights, in accordance with the law regulating free access to information of public importance and the law regulating personal data protection.

Data declassification which is in public interest

Article 26

The National Assembly, the President of the Republic and the Government may declassify specific documents, regardless of the level of classification, should that be in public interest or in order to perform international obligations.

Change of classification level and duration

Article 27

A change of the classification level shall mean to assign data a level of classification that is higher or lower than the level assigned to them up to that point, before the expiry of the time period from Articles 17 to 20 of this Law.

A change of the classification level and duration shall be implemented under the provisions of Articles 21 to 24 and Article 26 of this Law.

Information on change of classification level and declassification

Article 28

An authorised person shall inform the users of classified data or those who have access to them, in writing and without delay, of any change of the classification level and duration.

Foreign classified data

Article 29

A change of the classification level and duration, as well as the declassification of foreign classified data, shall be implemented under a concluded international agreement and established international obligations.

III CLASSIFIED DATA PROTECTION MEASURES

Classified data protection criteria

Article 30

A public authority shall, under this Law and any regulations adopted on the basis of this Law, establish a system of procedures and measures to protect classified data according to the following criteria:

1) the level of classification;
2) the nature of the document containing classified data;
3) classified data security threat assessment.

Types of protection measures

Article 31

A public authority shall apply general and special protection measures under law and regulations adopted under law, with a view to protecting classified data in its possession.

General protection measures

Article 32

General measures for the protection of classified data shall include:

1) determining the classification level;
2) assessing classified data security threat ;
3) establishing the manner of using and handling classified data;
4) designating a person responsible for keeping, using, exchanging and other forms of classified data processing;
5) designating a classified data controller, including his security clearance depending on the classification level;
6) determining special zones, buildings and premises intended for classified data and foreign classified data protection;
7) classified data handling control;
8) measures for the physical and technical protection of classified data, including the installation and set-up of technical means of protection, determination of a security zone and protection outside that zone;
9) protection measures for information and telecommunication systems;
10) crypto protection measures;
11) protection regime for jobs and formation posts, under any internal acts on job classification and systematisation;
12) establishing special educational and training programmes required for the protection of classified data and foreign classified data;
13) other general measures prescribed by law.

Special protection measures

Article 33

With a view to efficiently implementing general measures for classified data protection from Article 32 of this Law, special measures for classified data protection shall be brought under a Government act.

Some special protection measures can be regulated in more detail by an act of the competent minister or the head of a special organisation, under the Government act from paragraph 1 of this Article.

Responsibilities of data controller

Article 34

The data controller shall, under this Law and within his/her authority, undertake classified data protection measures, enable users to have direct access to classified data, issue copies of the

document containing classified data, keep records on users and be in charge of the exchange of classified data.

Keeping, transmitting and delivering classified data

Article 35

Classified data shall be kept in such a manner that only authorised users are allowed access to these data.

Classified data may be transmitted and delivered outside the premises of a public authority only in compliance with the prescribed security measures and procedures ensuring that classified data could be received only by a person who has a certificate for access to classified data and is entitled to receive them.

In transmitting and delivering classified data outside the premises of a public authority, security procedures and measures shall be determined according to the classification level assigned to such data, under law and in compliance with any regulation adopted under law.

The application of the prescribed measures of crypto protection shall be mandatory in transmitting and delivering classified data over telecommunication and information systems.

In transmitting and delivering classified data from paragraphs 3 and 4 of this Article, crypto protection measures shall be implemented under law.

Obligation to inform of loss, theft, damage, destruction or unauthorised disclosure of classified data and foreign classified data

Article 36

When an official, employee or a person performing specific tasks in a public authority, learns of any loss, theft, damage, destruction or unauthorised disclosure of classified data or foreign classified data, he/she shall inform the authorised person of a public authority thereof without delay.

The person from Article 35 paragraph 2 of this Law, who establishes that in transmitting and delivering classified data outside the premises of a public authority, there has been loss, theft, damage, destruction or unauthorised disclosure of classified data and foreign classified data, shall inform without delay the authorised person of the public authority that transmitted or delivered such classified data or foreign classified data.

The authorised person shall be bound to take, without delay, all measures required for determining the circumstances resulting in loss, theft, damage, destruction or unauthorised disclosure of classified data and foreign classified data, to assess the damage caused, as well as to take all necessary measures in order to redress damage and prevent any repeated loss, theft, damage, destruction or unauthorised disclosure of classified data and foreign classified data.

In the case described in paragraph 3 of this Article, the authorised person shall inform the Council Office of the measures undertaken.

IV ACCESS TO CLASSIFIED DATA

Access to classified data without certificate

Article 37

The President of the National Assembly, the President of the Republic and the Prime Minister shall have access to classified data and the right to use data and documents of any classification level without a certificate, by virtue of their office and for the purpose of performing tasks in their purview.

Access to classified data without security clearance and special powers and duties

Article 38

State authorities appointed by the National Assembly, heads of state authorities appointed by the National Assembly, judges of the Constitutional Court and judges, shall be authorised to access data of all levels of classification that they need in order to perform tasks in their purview, without security clearance.

Exceptionally, the persons from paragraph 1 of this Article shall have the right to access classified data marked as “TOP SECRET” and “SECRET”, with prior security clearance from Article 53 items 2) and 3) of this Law, should it be necessary to perform tasks in their purview, if such data are related to:

1) acts of preventing, discovering, investigating and prosecuting criminal offences, implemented by competent state authorities until the completion of investigation or prosecution;
2) manner of applying special procedures and measures in obtaining security and intelligence information in the given case;
3) members of the ministry of internal affairs and security services, who have secret identity, as long as it is necessary to protect the vital interests of these persons or members of their families (their life, health and physical integrity);
4) identity of the present and former associates of security services or third parties, as long as it is necessary to protect the vital interests of these persons or members of their families (life, health and physical integrity).

Persons who have access to classified data under this Law in any proceedings that they are conducting and otherwise, shall be authorised and bound to protect in every meaningful way and from everyone, classified data of which they learned, and to personally access the classified data from paragraph 2 of this Article.

Right of access to classified data granted to members of the competent National Assembly Committee

Article 39

Members of the National Assembly committee for monitoring and control in the field of defence and security shall have the right of access to classified data in connection with performing the task of monitoring and control under law.

Right of access to classified data marked as "RESTRICTED"

Article 40

Officials, employees and persons performing specific tasks in public authorities shall have access to classified data marked as "RESTRICTED".

The persons from paragraph 1 of this Article shall sign a statement to confirm that they shall handle classified data in accordance with law and other regulations.

Access to foreign classified data

Article 41

Access to foreign classified data shall be in accordance with this Law, any regulations adopted based on this Law, or in compliance with an international agreement concluded by the Republic of Serbia with a foreign country, international organisation or other international entity.

Natural and legal persons as users of classified data

Article 42

Natural and legal persons- users of classified data, have the right of access to classified data which are necessary for them to perform tasks in their purview, and whose classification level is determined in a certificate or permission for access to classified data (hereinafter: certificate).

As an exception to paragraph 1 of this Article, in case of extreme urgency, the person who has been issued a certificate or permission for access to classified data marked with the lower classification level may have insight into classified data marked with the next higher classification level.

The person from paragraph 2 of this Article shall be bound to sign a statement to confirm that he/she shall handle classified data in accordance with law and other regulations.

Statement and certificate

Article 43

Prior to issuing a certificate or permission, the person to whom a certificate is issued is bound to sign a statement to confirm that he/she shall handle classified data in accordance with law and other regulations.

If the person from paragraph 1 of this Article does not sign a statement, the procedure of issuing a certificate or permission shall be suspended.

A written statement shall be an integral part of the documentation based on which a certificate or permission has been issued.

Relief from obligation of keeping secrecy

Article 44

The person to whom a certificate or permission has been issued, may not use the classified data involved for any other purposes except for the purpose for which the certificate or permission has been issued.

The head of a public authority may, at the request of the competent authority, relieve a person of the obligation to keep data secret under a special decision envisaging, inter alia, measures to protect data secrecy, but only for the purpose and to the extent specified in the request of the competent authority, in accordance with law.

At the request of the competent authority, the head of a public authority may be relieved of the obligation to keep data secret by the authority which nominated, elected or appointed him/her, whereof the authority shall inform the Council Office.

Delivering classified data with obligation of keeping secrecy

Article 45

Classified data may be delivered to another public authority under a written authorisation issued by the authorised person of the public authority which marked the data involved as classified, unless a special law prescribes otherwise.

Classified data received from a public authority may not be delivered to another user without the consent of the authority which marked the data as classified, unless a special law prescribes otherwise.

Persons that perform specific tasks in the public authority to which the classified data from paragraph 1 of this Article have been delivered, shall be bound to act in accordance with the provisions of this Law and shall be under obligation to observe classification markings and to take measures to protect data secrecy.

Delivering classified data based on contractual relationship

Article 46

An authorised person may deliver classified data to another legal or natural person that offers services to a public authority on the basis of a contractual relationship, if:

1) the legal or natural person fulfils organisational and technical conditions for keeping classified data in accordance with this Law and regulations adopted under this Law;
2) the persons that perform contract tasks have undergone security clearance and have been issued certificates;
3) the persons from item 2) of this paragraph confirm by a written statement that they are familiar with this Law and other regulations governing the keeping of data secrecy and undertake to handle such classified data in accordance with those regulations;
4) access to classified data is absolutely necessary in order to perform the tasks envisaged by the contract involved.

Classified data protection measures stemming from paragraph 1 of this Article must be contained in the contract concluded between a public authority and a legal or a natural person in connection with the implementation of specific tasks.

The Government shall prescribe in more detail the manner and procedure of determining whether the conditions from paragraph 1 item 1) of this Article are fulfilled.

Records of classified data delivered to other users

Article 47

The controller of a public authority shall establish and keep updated records concerning classified data delivered to other users outside the public authority.

V PROCEDURE FOR ISSUING CERTIFICATE OR PERMISSION

Conditions for issuing certificate to natural persons

Article 48

A certificate shall be issued by the competent authority determined by this Law following a written request by a natural person, if the applicant is:

1) a citizen of the Republic of Serbia;
2) a person of age;
3) a person with legal capacity;

4) a person not sentenced to an unconditional prison sentence for a criminal offence prosecuted ex officio or a minor offence as envisaged by this Law;
5) a person who has undergone adequate security clearance.

Conditions for issuing certificate to legal persons

Article 49

A certificate is issued by the competent authority determined by this Law following a written request by a legal person submitted by a legal representative, if the applicant:

1) has a registered head office in the territory of the Republic of Serbia;
2) is engaged in an activity related to the interests laid down in Article 8 of this Law;
3) undergoes adequate security clearance;
4) is not undergoing liquidation or bankruptcy;
5) has not been pronounced a punitive measure prohibiting its business activity, or the penalty of termination of legal person, or a security measure prohibiting specific registered activities or tasks;
6) regularly pays taxes or contributions.

Issuing permission to foreign persons

Article 50

The competent authority may issue permission to foreign persons if:

1) they have an adequate security certificate issued by the foreign country whose citizens they are or in which they have the head office, or by the international organisation whose member they are;
2) the obligation of allowing access to classified data arises from a concluded international agreement.

Submitting a request

Article 51

A request for issuing a certificate or permission shall be submitted to the Council Office.

If the controller or other persons employed by a public authority apply for a certificate, the request from paragraph 1 of this Article shall be submitted by the head of the public authority.

If a legal person or persons employed by the legal person apply for a certificate, the request shall be submitted by the legal representative of the legal person.

A request for issuing a certificate to a person who is going to have access to classified data in connection with performing contract tasks for a public authority, shall be submitted by the public authority for which the contract tasks are performed.

Contents of request

Article 52

A request by a natural person for issuing a certificate shall contain: name and surname, residence, tasks he/she performs, reasons for requesting the certificate, as well as the classification level of the data for which the certificate is requested.

A request by a legal person for issuing a certificate shall contain: name of company, head office and business activity of the legal person, name, surname and residence of the legal representative of the legal person, reasons for requesting the certificate, as well as the classification level of the data for which the certificate is requested.

Apart from the information from paragraph 1 or 2 of this Article, a foreign person shall also submit the security certificate from Article 50 item 1) of this Law.

Security clearance

Article 53

Security clearance shall be implemented for access and use of classified data depending on the level of classification, namely:

1) basic security clearance, for data marked as “RESTRICTED” and “CONFIDENTIAL”;
2) full security clearance, for data marked as “SECRET”;
3) special security clearance, for data marked as “TOP SECRET”.

Authority responsible for security clearance

Article 54

Security clearance for access to classified data and documents marked as “TOP SECRET” and “SECRET” shall be conducted by the Security Information Agency of the Republic of Serbia.

Security clearance for access to classified data and documents marked as “CONFIDENTIAL” and “RESTRICTED” shall be conducted by the ministry responsible for internal affairs.

The Military Security Agency shall conduct security clearance for access to classified data and documents of any classification level for persons who need access to classified data and documents in order to discharge their functions and professional duties in the ministry responsible for defence and in the Army of the Republic of Serbia.

As an exception to paragraph 2 of this Article, security clearance for access to classified data and documents marked as “CONFIDENTIAL” and “RESTRICTED” for persons who need access to classified data and documents in order to discharge their functions or professional duties in the Security Information Agency, shall be conducted by the Security Information Agency.

Security clearance for access to classified data and documents marked as “SECRET” for persons who need access to classified data and documents of the mentioned classification level in order to discharge their functions and professional duties in the ministry responsible for internal affairs, shall be conducted, apart from the authority from paragraph 1 of this Article, by the ministry responsible for internal affairs.

The authorities responsible for security clearance from paragraphs 1 to 5 of this Article shall be bound to cooperate with each other in the security clearance procedure, particularly in the security clearance procedure for access to classified data marked as “TOP SECRET” and “SECRET”.

Cooperation with foreign countries and international organisations

Article 55

The authorities responsible for security clearance from Article 54 of this Law may cooperate in the security clearance procedure with agencies of foreign states, international organisations and other international entities responsible for security clearance, in accordance with international agreements concluded by the Republic of Serbia with a foreign country, international organisation or some other international entity, or with the regulations governing personal data protection in the Republic of Serbia.

Purpose of security clearance

Article 56

Security risks shall be assessed based on the applicant’s security clearance, particularly those arising from access to and use of classified data.

In conducting security clearance, the competent authority shall assess, in terms of security, the information contained in a completed security clearance questionnaire.

The competent authority shall collect, in connection with the details contained in the security clearance questionnaire, personal and other information from the person to whom the information is related, from other public authorities, organisations and persons, from registers, records, data bases and data collections kept under law.

Security clearance questionnaire

Article 57

In order to conduct security clearance, the Council Office shall submit a security clearance questionnaire to the applicant.

The applicant shall complete a basic security clearance questionnaire, and if a certificate is required for classified data marked as “TOP SECRET” and “SECRET”, the applicant shall also complete a special security clearance questionnaire.

The completed and signed questionnaire of the applicant shall at the same time constitute written consent for conducting security clearance and shall be marked as “RESTRICTED”.

Basic security clearance for natural persons

Article 58

The following information about the applicant shall be entered in a basic security questionnaire:

1) name and surname, as well as prior names and surnames;
2) personal identification number;
3) date and place of birth;
4) citizenship, prior citizenship and dual citizenship;
5) domicile and residence, and prior domiciles;
6) marital and family status;
7) information about persons sharing a household with the person to whom the security clearance questionnaire relates (their names and surnames, together with prior names and surnames, their dates of birth and their relation to the person undergoing security clearance);
8) name and surname, date of birth and address of relatives up to the lineal kin of the second degree and the collateral kin of the first degree, as well as of adoptive parents, foster parents, step-parents or nursing parents;
9) education and occupation;
10) information about previous employment;
11) information about military service;
12) information about criminal and minor offence punishment and ongoing criminal and minor offence proceedings;
13) medical reports concerning addiction disorders (alcohol, drugs, etc.) or mental disorders;
14) contacts with foreign security and intelligence services;
15) disciplinary procedures and disciplinary measures pronounced;
16) information about membership or participation in any organisations whose activities and objectives are prohibited;
17) information about responsibility for violating any regulations concerning data secrecy;
18) information about property rights or other real rights over real estate, information about property rights over other things entered in the public register, as well as information about the annual tax on total income for the previous year;
19) previous security clearance checks.

Basic security questionnaire for legal persons

Article 59

The following information about the applicant shall be entered in a basic security questionnaire for legal persons:

1) company name and seat, as well as previous names and seats;
2) registration number of legal person and tax identification number;
3) name and surname of representative;
4) date and place of incorporation;
5) information about organisational units, branches, sister companies and other forms of affiliation;
6) origin of seed capital, including any changes in the last three years;
7) number of employees;
8) number of employees for whom the certificate is required and type of tasks they perform;
9) information about convictions for any criminal offence, economic transgression and offence committed by a legal person and persons responsible employed by the legal person, as well as information about any ongoing criminal offence proceedings, economic transgression or offence proceedings against the legal person;
10) information about contacts with foreign security and intelligence services;
11) information about participation in any organisations whose activities and objectives are prohibited;
12) information about responsibility for violating any regulations concerning data secrecy;
13) information about a previous security clearance check;
14) information about property rights or other real rights over real estate, information about property rights over other things entered in the public register, as well as information about the annual financial statement for the previous year in accordance with the law regulating accounting and auditing.

In addition to the questionnaire from paragraph 1 of this Article, the representative of the legal person shall submit a completed basic security questionnaire for natural persons.

Special security questionnaire

Article 60

For the security clearance laid down in Article 53 items 2) and 3) of this Law, apart from completing a basic security questionnaire, it is also necessary to complete a special security questionnaire.

The following information shall be entered in a special security questionnaire:

1) information about military service and service in paramilitary formations of a foreign country;
2) other information and facts, apart from the facts mentioned in Articles 58 and 59, making the legal or the natural person susceptible to influence and pressure constituting a security risk;
3) information about debts arising from financial liabilities or assumed guarantees.

Subject of security clearance and questionnaire form

Article 61

Information from the questionnaire from Articles 58 to 60 of this Law shall be the subject of adequate security clearance.

Forms of the questionnaire from paragraph 1 of this Article shall be prescribed by the Government at the proposal of the Council Office.

Special security clearance

Article 62

Special security clearance shall be conducted when a certificate or permission is required for data marked as "TOP SECRET".

Special security clearance shall include, in addition to security check within full security clearance, the checking of facts, circumstances and events concerning the applicant's private life, at least in the last ten years from the day of applying for the certificate, which, if any, would constitute reason to doubt the applicant's trustworthiness and reliability, particularly if his/her activities are in contravention of the interests of the Republic of Serbia, or if he/she is connected with foreign persons who might jeopardise the security and international interests of the Republic of Serbia.

Security clearance deadline

Article 63

The competent authority shall be bound to conduct security clearance within the following time periods, as of the day of reception of a completed questionnaire:

1) up to 30 days, for basic security clearance;
2) up to 60 days, for full security clearance;
3) up to 90 days for special security clearance.

As an exception, should there be justified reasons for that, the deadlines from paragraph 1 items 2) and 3) of this Article may be extended at most for the time period determined in these items.

In the case described in paragraph 2 of this Article, the competent authority shall be bound to inform the head of the public authority that submitted a request for security clearance, as well as the Council Office, of the deadline extension.

If security clearance is not completed within the time periods established in paragraphs 1 and 2 of this Article, it shall be considered that the applicant's access to secret data poses no security risk.

Temporary certificate

Article 64

For a public authority to perform pressing activities and tasks in order to prevent or redress damage, the Council Office Director may issue, exceptionally and before the completion of security clearance, a temporary certificate to a person for access to specific classified data, if it is assessed from the submitted security clearance questionnaire that there are no security doubts.

The person from paragraph 1 of this Article is bound to confirm in a written statement that he/she shall handle the classified data entrusted to him/her under this Law and other regulations governing the keeping and handling of secret data.

The temporary certificate from paragraph 1 of this Article shall be valid until the completion of the certificate issuing procedure.

Submitting reports on security clearance results

Article 65

The authorities responsible for security clearance from Article 54 of this Law shall submit to the Council Office a report on the results of security clearance or special security clearance, including a completed security clearance questionnaire, with a recommendation for issuing or denying the certificate.

The report from paragraph 1 of this Article shall not state the sources of security clearance.

The report and recommendation from paragraph 1 of this Article shall be marked as "CONFIDENTIAL".

Decision and additional check

Article 66

The Council Office shall pass a decision on issuing a certificate within 15 days from the day of submitting the report and the recommendation from Article 65 paragraph 1 of this Law, i.e. from the expiry of the deadline for conducting security clearance from Article 63 of this Law.

If the report is incomplete or contains no recommendation, the Council Office shall pass a decision based on the submitted report.

As an exception, if it is impossible to conclude from the report on security clearance results and from the recommendation for issuing a certificate whether the conditions for issuing a certificate, as prescribed by law, to a natural or legal person have been fulfilled, or whether after the conducted security clearance there have been significant changes of the checked data that might affect issuing a certificate, the Council Office shall request the competent authority from Article 54 of this Law to conduct an additional security check or to supplement the report and make a new recommendation, within an additional time period of 30 days at the latest.

Exceptions

Article 67

As an exception to Article 66 of this Law, for persons who need access to classified data in order to discharge their functions and professional duties in the security services of the Republic of Serbia, a decision on issuing a certificate for access to the classified data in possession of a security service, shall be passed by the head of the service from Article 54 paragraphs 3 and 4 of this Law.

Submitting a decision

Article 68

The Council Office shall submit the decision to the head of the public authority requesting a certificate to be issued and to the person for whom the certificate was requested.

Denying a request

Article 69

The Council Office shall deny a request for issuing a certificate by passing a decision thereon, if it is established based on a security clearance report or an additional security clearance report that:

1) the applicant stated untrue and incomplete information in a basic or special security clearance questionnaire;
2) the applicant does not fulfil the conditions from Articles 48 to 50 of this Law for issuing a certificate or permission;
3) the applicant has not met the conditions for undertaking the prescribed protection measures for classified data;
4) there is a security risk arising from access and use of classified data by the applicant.

The rationale for a decision denying a certificate shall not contain any information considered to be secret for the purposes of this Law, nor shall it state the sources of security clearance.

Adequate implementation

Article 70

Unless it is otherwise prescribed by this Law, the provisions of the law regulating general administrative procedure shall apply to the procedure for issuing a certificate or permission.

Administrative dispute

Article 71

An appeal may be lodged with the minister responsible for justice against the decision of the Council Office from Article 66 paragraph 1 of this Law.

The provisions of the law governing administrative procedure shall apply to decision upon appeal.

The decision of the minister responsible for justice shall be final and an administrative dispute may be instituted against it.

Contents, form and submitting of certificate

Article 72

The contents, form and manner of submitting a certificate shall be prescribed by the Government, at the proposal of the Council Office.

The Council Office shall submit a certificate and acquaint the user with the conditions prescribed for handling classified data, as well as with legal and other consequences of their unauthorised use.

On the occasion of receiving the certificate, the user shall sign the certificate and a statement confirming that he/she is familiar with the provisions of this Law and other regulations governing classified data protection, and that he/she shall use classified data in accordance with law and other regulations.

Termination of certificate validity

Article 73

The validity of a certificate shall be terminated:

1) upon expiry of the time period for which it was issued;
2) upon the termination of office from Article 38 of this Law;
3) upon termination of duties and tasks within the purview of the persons from Article 40 of this Law;

4) under a decision of the Council Office brought within the verification procedure for the issued certificate;
5) by death of the natural person or by termination of the legal person that has been issued a certificate.

Termination of certificate validity by lapse of time

Article 74

A certificate issued for data and documents marked as “TOP SECRET” shall be valid for three years.

A certificate issued for data and documents marked as “SECRET” shall be valid for five years.

A certificate issued for data and documents marked as “CONFIDENTIAL” shall be valid for ten years.

A certificate issued for data and documents marked as “RESTRICTED” shall be valid for fifteen years.

Extension of certificate validity

Article 75

The Council Office shall inform the holder of a certificate in writing that he/she may apply for the extension of certificate validity, six months before the expiry of its validity at the latest.

In addition to applying for the extension of certificate validity from paragraph 1 of this Article, the applicant shall inform the Council Office of any changes of the data contained in the previously submitted security clearance questionnaire, accompanied with relevant evidence, and the competent authority from Article 54 of this Law shall conduct repeated security clearance.

The provisions of Article 48 to 63 and Article 66 of this Law shall apply to the repeated clearance procedure from paragraph 2 of this Article, unless an international agreement stipulates otherwise.

Temporary ban on access rights

Article 76

If a disciplinary procedure has been instituted against a person to whom a certificate has been issued due to the grave violation of official duty, grave violation of military discipline or grave violation of professional obligations and duties, or if criminal proceedings have been launched due to reasonable doubt that the person has committed a criminal offence to be prosecuted ex officio, or minor offence proceedings for a minor offence envisaged by this Law, the head of the public authority may bring a decision temporarily banning that person from accessing classified data, pending the completion of the proceedings.

Certificate check

Article 77

Should it be established that the person to whom a certificate has been issued fails to use or keep classified data according to this Law and other regulations, or that he/she does not fulfil the conditions for issuing the certificate any longer, the Council Office shall adopt a decision on termination of certificate validity before the expiry of validity period, or a decision on limiting the rights of access to classified data assigned a specific level of classification.

The rationale of the decision from paragraph 1 of this Article shall not contain any data that are considered secret for the purposes of this Law.

The decision of the Council Office from paragraph 1 of this Article shall be final and administrative dispute may be instituted against it.

Issuing permission to foreign persons

Article 78

The Council Office shall issue permission to a foreign person under a concluded international agreement.

Upon receiving the application, the Council Office shall check through international channels if the applicant has been issued a security certificate by the foreign state whose citizen he/she is or in which the applicant has a registered office, or by the international organisation whose member the applicant is.

Permission shall be issued only for access to data and documents specified in an international agreement concluded by the Republic of Serbia with a foreign state, international organisation or another international entity.

The provisions of this Law concerning certificate issuance shall apply to issuing permission to foreign persons.

Official records and other data related to certificate and permission

Article 79

The Council Office shall keep a single central register of issued certificates and permissions, of decisions on issuing certificates and permissions, decisions on denying certificates and permissions, decisions on certificate or permission validity extension, decisions on limitation or termination of certificate and permission validity, as well as signed statements of the persons to whom a certificate or permission has been issued.

The Council Office shall keep certificate or permission applications, security clearance questionnaires and security clearance reports with recommendations.

Security clearance records

Article 80

The authority responsible for the security clearance from Article 54 of this Law shall keep security clearance records and security clearance documents with a copy of the report and recommendation.

Security clearance information may be used only for the purposes for which it has been collected.

Application of personal data protection regulations

Article 81

A person shall have the right to have insight into his/her security clearance information collected under this Law, as well as other rights based on that insight in accordance with the law regulating personal data protection, except for information that would reveal the methods and procedures applied in collecting the information involved, or identify the information sources within security clearance.

Records of public authorities

Article 82

A public authority shall keep records of decisions concerning certificates issued for persons that discharge a function, are employed or perform tasks in a public authority.

The certificate decision from paragraph 1 of this Article shall be kept in a separate part of the person's employment file, and the information from the decision may be used only in connection with the implementation of the provisions of this Law or a regulation brought based on this Law.

More detailed regulation of contents, form and manner of keeping records

Article 83

The contents, form and manner of keeping records, as well as the time period of data keeping from Articles 79, 80 and 82 of this Law shall be prescribed by the Government, at the proposal of the Council Office.

VI CONTROL AND OVERSIGHT

1. Internal control

Article 84

The head of a public authority shall be responsible for internal control of the implementation of this Law and regulations adopted based on this Law.

A special post shall be allocated in the ministry responsible for internal affairs, the ministry responsible for defence and in the Security Information Agency, and, as necessary, in other public authorities, for internal control and other professional tasks concerning secret data classification and protection, or else an existing organisational unit within the ministries or the agency shall be entrusted with performing the mentioned activities and tasks.

Objective of internal control

Article 85

Internal control shall ensure the regular monitoring and assessment of particular activities, as well as of the activity of a public authority as a whole, in connection with the implementation of this Law and regulations and measures adopted based on this Law.

The head of a public authority shall implement internal control, directly or through an authorised person, through adequate verification and consideration of submitted reports.

2. The Council Office

Status of the Council Office

Article 86

The Council Office is a Government agency that has the capacity of legal person, and is responsible for specific activities concerning the implementation of this Law and the monitoring of its implementation, as well as for oversight of the implementation of this Law.

Competence of the Council Office

Article 87

Under this Law, the Council Office shall:

1) act upon requests for the issuance of certificates and permissions;
2) ensure the implementation of relevant standards and regulations in the field of secret data protection;
3) attend to the implementation of assumed international obligations and international agreements concluded between the Republic of Serbia and other states or international agencies and organisations in the field of secret data protection, and cooperate with relevant agencies of foreign states and international organisations;

4) develop and keep a central register of foreign classified data;
5) propose a security questionnaire form;
6) propose a recommendation, certificate and permission form;
7) keep records on issued certificates or permissions, as well as records on denied certificates or permissions;
8) organise the training of secret data users in compliance with relevant standards and regulations;
9) propose a plan of secret data protection to the Government, in case of emergency and in urgent circumstances;
10) declassify data in compliance with the provisions of this Law;
11) perform tasks concerning secret data protection, upon the termination of public authorities without a legal successor;
12) cooperate, within its competence, with public authorities in implementing this Law;
13) perform other tasks envisaged by this Law and regulations adopted based on this Law.

The Director of the Council Office shall submit to the Government an annual report on activities in the purview of the Council Office.

Taking over classified data

Article 88

The Council Office shall take over the classified data of public authorities that ceased to exist and do not have a legal successor, i.e. charge another public authority to keep and use the data involved.

Director of the Council Office

Article 89

The Government shall appoint and relieve of duty the Director of the Council Office, upon obtaining an opinion of the National Security Council.

The Director of the Council Office shall be appointed for a period of five years.

The same person may be appointed Director of the Council Office twice at most.

A person who meets general requirements for employment in state authorities, who has university-level education and at least ten years of work experience in the field of security, shall be appointed Director of the Council Office.

The Director of the Council Office may not be a member of any political party.

The Director of the Council Office shall be accountable to the Government and the Prime Minister.

The Director of the Council Office shall be a civil servant holding an office.

Termination of office

Article 90

The Director of the Council Office shall terminate his office for the reasons established by the law regulating the rights and obligations of civil servants.

The Director of the Council Office shall be relieved of office for the reasons established by the law regulating the rights and obligations of civil servants, as well as if he/she becomes a member of a political party.

Deputy Director of the Council Office

Article 91

The Council Office shall have a Deputy Director appointed by the Government, at the proposal of the Director of the Council Office.

The Deputy Director shall be appointed for a period of five years.

The Deputy Director may be a person who meets general requirements for employment in state authorities, who has university-level education and at least nine years of work experience in the field of secret data protection.

The Deputy Director may not be a member of any political party.

The Deputy Director shall be a civil servant holding an office.

The Deputy Director shall discharge the function of Director of the Council Office in his/her absence, in case of his/her death, expiry of office, relief from office, as well as temporary or permanent incapacity to perform the duties of Director of the Council Office.

The Deputy Director shall terminate his/her tenure of office for the reasons established by the law regulating the rights and obligations of civil servants.

The Deputy Director shall be relieved of duty for the reasons established by the law regulating the rights and obligations of civil servants, as well as if he/she becomes a member of a political party.

Act on internal job organisation and allocation and increase of salary

Article 92

The Director of the Council Office shall adopt an act on the internal job organisation and allocation, to be approved by the Government upon obtaining an opinion of the National Security Council.

A person who is in charge of secret data protection may be employed by the Council Office if he/she has undergone special security clearance.

Regulations applying to the employment of civil servants and employees shall apply to the employment of the Council Office Director, the Deputy Director and the employees in the Council Office in charge of secret data protection.

Due to the specific working conditions, the complexity and nature of work, the Council Office Director, the Deputy Director and the employees in the Council Office in charge of secret data protection, may have their salary increased by up to 20% as compared to the salary of a civil servant and employee whose jobs are in the same classification group or in the same occupational group as the jobs of civil servants and employees in charge of secret data protection, under a Government act.

Obligations of the Council Office in connection with foreign classified data

Article 93

The exchange of classified data with foreign states and international organisations shall be carried out through the Council Office, unless it is otherwise prescribed by a special law or an international agreement.

Central register of foreign classified data

Article 94

The Council Office shall establish, keep and secure a central register of foreign classified data and documents.

The public authority that has received foreign classified data and documents in accordance with a special law or an international agreement concluded by the Republic of Serbia with a foreign state, international organisation or other international entity, shall establish, keep and secure a special register of foreign classified data.

The public authority shall submit to the Council Office, at least once a year, a report containing figures on the exchange of classified data with a foreign state or an international organisation.

Delivering and receiving information

Article 95

The Council Office shall inform a foreign state or an international organisation of the security of foreign classified data received within international exchange.

The Council Office shall receive information from a foreign state or an international organisation concerning the security of the classified data delivered by the Republic of Serbia within international exchange.

Exchange of information without concluding an international agreement

Article 96

In extremely unfavourable political, economic or defence and security circumstances for the Republic of Serbia, and if it is necessary in order to protect the interests from Article 8 paragraph 2 of this Law, the Council Office shall, at the request of a public authority, exchange classified data with a foreign state or an international organisation without previously concluding an international agreement.

3. Oversight

Article 97

The Ministry responsible for justice (hereinafter: the Ministry) shall conduct oversight of the implementation of this Law and regulations adopted under law.

In implementing oversight and in accordance with this Law, the Ministry shall:

1) monitor the situation in the field of secret data protection;
2) draw up regulations required for the implementation of this Law;
3) give an opinion on draft regulations in the field of secret data protection;
4) propose to the Government the contents, form and manner of keeping classified data records, as well as regulations governing the security questionnaire form or the recommendation, certificate and permission form;
5) impose measures for promoting classified data protection;
6) supervise the implementation of the criteria on marking the classification level and conduct other supervision activities under the provisions of this Law;
7) press criminal charges, submit requests for initiation of minor offence proceedings and propose initiation of other proceedings on account of the violation of the provisions of this Law, in accordance with law;
8) cooperate, within its competence, with public authorities in implementing this Law;
9) perform other tasks envisaged by this Law and regulations adopted based on this Law.

The minister responsible for justice shall submit an annual report on activities concerning the implementation of this Law and the supervision of its implementation, to the National Assembly committee responsible for oversight and control in the field of defence and security.

The ministry shall, within its oversight activities, supervise the implementation of measures aimed at security, use, exchange and other forms of classified data processing, without previously informing the public authority, authorised person, controller or user of classified data.

The ministry shall perform the tasks from paragraphs 1, 2 and 4 of this Article, through authorised persons who have previously undergone special security clearance.

The authorised persons from paragraph 5 of this Article shall conduct oversight through adequate implementation of regulations on inspection control.

The authorised persons from paragraph 5 shall be entitled to an official identification card.

Due to the specific working conditions, the complexity and nature of work, the authorised persons from paragraph 5 of this Article may have their salary increased by up to 20% as compared to the salary of a civil servant and employee in the ministry responsible for justice, who is in charge of the oversight of activities of judicial authorities, under a Government act.

The minister responsible for justice shall adopt a more detailed regulation on official identification cards and the manner of work of authorised persons.

VII PUNITIVE PROVISIONS

Criminal offence

Article 98

If a person should, without being authorised to do so, communicate, deliver to or make available for an unauthorised person any data or documents entrusted to him/her, or of which he/she has learnt otherwise, or if a person should obtain data or documents constituting secret data marked as "RESTRICTED" or "CONFIDENTIAL", as established by this Law,

the person shall be sentenced to prison term of three months to three years.

If the offence from paragraph 1 of this Article has been committed in connection with data marked as "SECRET" under this Law,

the offender shall be sentenced to prison term of six months to five years.

If the offence from paragraph 1 of this Article has been committed in connection with data marked as "TOP SECRET" under this Law,

the offender shall be sentenced to prison term of one to ten years.

If the offence from paragraphs 1 to 3 of this Article has been committed for gain or with a view to releasing or using classified data in a foreign country, or if it has been committed during a state of war or emergency,

the offender shall be sentenced to prison term of six months to five years for the offence from paragraph 1 of this Article, one to eight years for the offence from paragraph 2, and five to fifteen years for the offence from paragraph 3.

If the offence from paragraphs 1 to 3 of this Article has been committed out of negligence,

the offender shall be sentenced to prison term of up to two years for the offence from paragraph 1 of this Article, three months to three years for the offence from paragraph 2, and six months to five years for the offence from paragraph 3.

Minor offence liability of responsible persons in public authorities

Article 99

The responsible person in a public authority shall be fined between 5,000 and 50,000 dinars if he/she:

1) marks data and documents as secret (Article 8 paragraph 2), even though they are obviously not related to protected interests;
2) transfers authority for data classification to a third person (Article 9 paragraph 3);
3) assigns classified data contained in a document an inadequate classification level (Article 11 paragraph 2);
4) passes a decision on data classification without a rationale (Article 11 paragraph 4);
5) fails to declassify data upon the date or event after which data should be declassified (Articles 17 and 18);
6) fails to declassify data upon the expiry of a legal time period for declassification (Article 19);
7) fails to conduct periodical classification assessments (Article 22);
8) fails to declassify data on the basis of a decision of the Commissioner for Information of Public Importance and Personal Data Protection or based on the ruling of the competent court (Article 25);
9) changes the classification level of a document in contravention of the provision of Article 27 of this Law;
10) fails to inform public authorities of any changes of the classification level and declassification (Article 28);
11) fails to prescribe, develop and supervise general and special measures of classified data protection, corresponding to their classification level (Articles 32 and 33);
12) fails to submit for signature to the person to whom a certificate for access to classified data has been issued, a statement confirming that the person is acquainted with the regulations governing secret data protection (Article 42 paragraph 3);
13) delivers classified data to legal and natural persons in contravention of the provision of Article 46 of this Law;
14) fails to keep records of decisions on certificates issued for access to classified data (Article 82 paragraph 1);
15) fails to keep decisions concerning access to classified data in a separate part of the employment file (Article 82 paragraph 2);

16) fails to organise the internal control of secret data protection (Article 84 paragraph 1);
17) fails to undertake measures to establish, keep and secure a special register of foreign classified data (Article 94 paragraph 2).

Minor offence liability of classified data controllers

Article 100

The controller of classified data who fails to undertake classified data protection measures (Article 34) shall be fined between 5,000 and 50,000 dinars for that offence.

VIII TRANSITIONAL AND FINAL PROVISIONS

Article 101

The National Security Council Office, established under Article 8 of the Law on Basic Regulation of Security Services of the Republic of Serbia ("Official Gazette of the Republic of Serbia", No. 116/07), shall proceed with its work on the day of entry into force of this Law, under the name of the Office of the Council for National Security and Protection of Secret Data.

The Director of the National Security Council Office, appointed under the law from paragraph 1 of this Article as of the day of entry into force of this Law, shall continue to discharge the function of Director of the Office of the Council for National Security and Protection of Secret Data, until the expiry of his/her term of office.

Appointment of Deputy Director

Article 102

The Government shall appoint Deputy Director of the Council Office within three months from the day of entry into force of this Law.

Adoption of acts on internal job classification and systematisation and takeover of employees

Article 103

An act on internal job classification and systematisation in the Council Office shall be adopted within 60 days from the day of entry into force of this Law.

The Council Office shall take over the necessary number of employees from other public authorities performing tasks in the field of data secrecy, within 90 days from the day of adopting the act from paragraph 1 of this Article.

Adoption of by-laws

Article 104

By-laws envisaged by this Law and passed by the Government shall be adopted within six months from the day of entry into force of this Law.

By-laws envisaged by this Law and passed by other public authorities shall be adopted within one year from the day of entry into force of this Law.

The provisions of the existing by-laws that are not in contravention of the provisions of this Law shall be implemented pending the adoption of the by-laws from paragraphs 1 and 2 of this Article.

Reconsideration of existing classification markings

Article 105

As of the day of entry into force of this Law, data and documents assigned a classification level based on earlier regulations, shall keep the type and level of classification assigned under such regulations.

The heads of public authorities shall reconsider the classification markings of the data and documents from paragraph 1 of this Article within two years from the day of entry into force of this Law, under the provisions of this Law.

Harmonisation of by-laws and issuance of certificates to employees in public authorities

Article 106

Public authorities shall be bound to harmonise their organisation with the provisions of this Law within one year from the day of entry into force of this Law.

Public authorities shall be bound to ensure that all their employees who need to have access to classified data in order to perform their professional duties and functions, should be issued certificates for access to classified data, under this Law, within two years from the day of entry into force of this Law.

Harmonisation of international agreements

Article 107

The competent authorities of the Republic of Serbia shall reconsider the provisions of the existing international agreements concluded by the Republic of Serbia in the field of secret data protection, within two years from the day of entry into force of this Law, and initiate a procedure to amend international agreements as necessary.

Implementation of existing laws with regard to classification and protection of secret data

Article 108

The provisions of the existing laws governing the work of public authorities, inasmuch as they are related to the system of classification and protection of classified data and foreign classified data, which are not in contravention of the provisions of this Law, shall be applied until the date on which this Law takes effect.

Laws and other regulations that cease to have effect

Article 109

On the date on which this Law takes effect, the following shall cease to have effect:

1) Article 123 of the Defence Law ("Official Gazette of the Republic of Serbia", No. 116/07);
2) the provisions of Chapter VI- Security and Protection Measures, from Articles 67 to 86 of the Defence Law ("Official Gazette of the Federal Republic of Yugoslavia", No. 43/94, 11/95, 28/96, 44/99 and 3/02 and "Official Gazette of the Republic of Serbia", No.116/07 –other law).
3) Article 45 paragraphs 2 to 4 of the Law on Personal Data Protection ("Official Gazette of the Republic of Serbia", No. 97/08).

Entry into force

Article 110

This Law shall enter into force on the eighth day from its publication in the Official Gazette of the Republic of Serbia, and shall take effect as of 1 January 2010.