L A W
ON PERSONAL DATA PROTECTION

I. BASIC PROVISIONS

Scope

Article 1

This Law shall set out the conditions for personal data collection and processing, the rights and protection of the rights of persons whose data are collected and processed, limitations to personal data protection, proceedings before an authority responsible for data protection, data security, data filing, data transfers outside the Republic of Serbia and enforcement of this Law.

Every natural person shall be entitled to personal data protection regardless of their nationality and residence, race, age, gender, language, religion, political and other affiliations, ethnicity, social background and status, wealth, birth, education, social position or any other personal characteristic.

The duties of personal data protection shall be carried out by the Commissioner for Information of Public Importance and Personal Data Protection (hereinafter referred to as the Commissioner), as an autonomous public authority who exercises his/her powers independently.

Purpose

Article 2

The purpose of this Law is to enable every natural person to exercise and have recourse to protection of their right to privacy and other rights and freedoms in the context of personal data protection.

Definition of Terms used in this Law

Article 3

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

1) “personal data” means any information relating to a natural person, regardless of the form of its presentation or the medium used (paper, tape, film, electronic media etc.), regardless on whose order, on whose behalf or for whose account such information is stored, regardless of the date of its creation or the place of its storage, regardless of the way in which such information is learned (directly, by listening, watching etc., or indirectly, by accessing a document containing the information etc.) and regardless of any other characteristic of such information (hereinafter referred to as data);

2) “natural person” means any data subject identified or identifiable on the basis of his/her proper name, unique personal identification number, address code or any other distinguishing feature of his/her physical, psychological, spiritual, economic, cultural or social identity (hereinafter referred to as person);

3) “data processing” means any action taken in connection with data, including: collection, recording, transcription, multiplication, copying, transmission,

searching, classification, storage, separation, crossing, merging, adaptation, modification, provision, use, granting access, disclosure, publication, dissemination, recording, organizing, keeping, editing, disclosure through transmission or otherwise, withholding, dislocation or other actions aimed at rendering the data inaccessible, as well as other actions carried out in connection with such data, regardless whether those actions are automated, semi-automated or otherwise performed (hereinafter referred to as processing);

4) "public authority" means a state authority, a territorial autonomy or local self-government authority or another authority or organization vested with public powers;

5) "data controller" means a natural person, legal entity or public authority responsible for data processing (hereinafter referred to as controller);

6) "data file" means any set of data undergoing automated or non-automated processing and available on personal grounds, case-related grounds or any other grounds, regardless of the mode of their filing and place of their storage;

7) "data user" means any natural person, legal entity or public authority authorized by virtue of the law or on the basis of a person's consent to use data (hereinafter referred to as user);

8) "data processor" means any natural person, legal entity or public authority to whom/which a controller delegates certain processing-related duties under the law or on the basis of a contract (hereinafter referred to as processor);

9) "in writing" includes also electronically, subject to the provisions of the law governing electronic signature;

10) "Central Data File Register" (hereinafter referred to as the Central Register) means a record comprising a register of data files and a catalogue of data files, managed by the Commissioner.

Application of the Law

Article 4

The provisions of this Law shall apply to any automated processing, as well as to processing incorporated in non-automated data files.

Data excluded from the Scope of the Law

Article 5

Save where a person's contrary interests manifestly prevail, certain provisions of this Law pertaining to processing requirements and to the rights and responsibilities in connection with processing shall not apply to the processing of:

1) Data available to everyone and published in mass media or publications or accessible in archives, museums and other similar organizations;

2) Data processed for family purposes and other personal purposes which are unavailable to third parties;

3) Data on members of political parties, associations, trade unions and other forms of alliances processed by such organizations, provided that the member

concerned has given his/her consent in writing to waive the application of certain provisions of this Law to his/her personal data for a specified period of time, which however cannot exceed the term of his/her office;

4) Data published on oneself by a person capable of taking care of his/her interests.

Processing for Historical, Statistical or Research and Development Purposes

Article 6

Data collected and processed for other purposes can be processed solely for historical, statistical or research and development purposes, provided they are not used in decision-making or in the taking of measures against the person concerned and only if adequate safeguards are in place.

Safeguards for the protection of data archived solely for historical, statistical or research and development purposes shall be set out in a special regulation.

Controller appointed under Special Regulation

Article 7

If a special regulation governs the purpose and manner of processing, the controller can be appointed pursuant to such regulation.

II. PROCESSING REQUIREMENTS

Inadmissibility of Processing

Article 8

Processing shall not be allowed:

1) If a natural person did not give his/her consent to processing, i.e. if processing is carried out without legal authority;

2) If processing is done for purposes other than those specified, regardless whether it is based on a person’s consent or on statutory powers for data processing without consent;

3) If the purpose of processing is vaguely defined, modified, inadmissible or already achieved;

4) If the data subject is identified or identifiable even after the purpose of such processing is achieved;

5) If the processing method is inadmissible;

6) If the processed data is unnecessary or unsuitable for the purpose of processing;

7) If the number or type of data processed is disproportionate taking into account the purpose of processing;

8) If the data are inaccurate and incomplete, i.e. if they are not based on a credible source or are outdated.

Decision made by Automated Processing

Article 9

Any decision producing legal consequences for a person or compromising his/her position cannot be based solely on data processed automatically and used in the assessment of some specific characteristic of his/hers (work ability, reliability, creditworthiness etc.).

Decisions referred to in paragraph 1 of this Article can be made where expressly provided for by the law or when a person's request relating to contract execution or performance is adopted, provided that adequate safeguards are put in place.

In cases referred to in paragraph 2 of this Article, the person concerned must be informed of the automated data processing and the decision-making process.

Processing with Consent

Article 10

Consent to data processing is deemed to be valid if given by a person who has received prior information from the controller within the meaning of Article 15 of this Law.

A person's valid consent can be given in writing of verbally for the record.

Consent may be given through a proxy.

A proxy's power of attorney shall be notarized, unless provided otherwise by the law.

For persons incapable of giving their own consent, such consent shall be given by their appointed representatives or guardians.

Consent for processing of data on deceased persons may be given by the spouse, children above 15 years of age, parents, siblings, legal heirs or persons appointed for that purpose by the deceased.

Withdrawal of Consent

Article 11

Consent may be withdrawn.

A person's valid withdrawal of consent can be made in writing or verbally for the record.

In case of withdrawal, the person who previously gave his/her consent shall reimburse the controller for any and all justifiable costs incurred and damage sustained, in accordance with the regulations pertaining to damage liability.

Data processing shall not be allowed once the consent has been withdrawn.

Processing without Consent

Article 12

Processing without consent shall be allowed in the following cases:

1) To achieve or protect vital interests of the data subject or a third party, in particular their life, health and physical integrity;

2) For the purpose of discharging duties laid down by a law, an enactment adopted pursuant to a law or a contract concluded between the person concerned and the controller, as well as for the purpose of contract preparation;

3) In other cases envisaged by this Law or another regulation adopted pursuant to this Law, for the purpose of achieving a prevailing justifiable interest of the person concerned, the controller or a user.

Processing by Public Authorities

Article 13

Public authorities shall process data without the consent of the person concerned if such processing is necessary for them to perform duties within their spheres of competence as defined by a law or another regulation with a view to achieving the interests of national or public safety, national defence, crime prevention, detection, investigation and prosecution, economic or financial interests of the state, protection of health and ethical norms, protection of rights and freedoms and other public interests, while processing in all other cases shall require the consent in writing from the person concerned.

Data Collection

Article 14

Data shall be collected from data subjects and from public authorities authorized under the law to collect such data.

Data may also be collected from third parties if:

1) envisaged by a contract concluded with a data subject;

2) envisaged by a law or another regulation passed pursuant to a law;

3) necessary taking into account the nature of the task;

4) data collection from a data subject is time-consuming or requires disproportionately high resources;

5) data are collected for the purpose of achieving or protecting vital interests of a data subject, in particular his/her life, health and physical integrity.

Notification of Data Processing

Article 15

The controller who collects data from data subjects or from third parties shall, before data collection, inform the data subject or the third party of:

1) His/her identity, i.e. name and address or business name, or the identity of another person responsible for data processing under the law;

2) The purpose of data collection and subsequent processing;

3) The manner in which data will be used;

4) The identity or categories of persons who will use data;

5) The mandatory nature and legal grounds or else the voluntary nature of data provision and processing;

6) The right to withdraw one's consent to processing and the legal consequences in the event of withdrawal;

7) The data subject's rights in case of unlawful processing;

8) Other circumstances the withholding of which from a data subject or a third party would be contrary to conscientious treatment.

The obligation referred to in paragraph 1 of this Article shall not pertain where such information, taking into account the specific circumstances of a case, is impossible or obviously unnecessary or unsuitable, in particular if the data subject or the third party is already informed or if the data subject is unavailable.

A controller who collected data on a data subject from a third party shall inform the data subject of the requirements of paragraph 1 of this Article without delay or at the time of first processing at the latest, save where such informing, taking into account the circumstances of the case, is impossible or obviously unnecessary or unsuitable, in particular if the data subject is already informed or if the data subject is unavailable or if collection and processing of data obtained from a third party is provided for under the law.

In cases referred to in paragraph 3 of this Article, the controller shall inform the data subject as soon as reasonably possible or when required by the data subject.

The information referred to in paragraph 1 of this Article shall be provided in writing if the consent to processing is given in writing, except when the data subject or third person agrees to receive information verbally.

The controller shall notify the data subject and the data user of any modification, amendment or deletion of data without delay, and in any case not later than 15 days of the date of such modification, amendment or deletion.

Particularly Sensitive Data

Article 16

Data relating to ethnicity, race, gender, language, religion, political party affiliation, trade union membership, health status, receipt of social support, victims of violence, criminal record and sexual life shall be processed on the basis of informed consent of data subjects, save where the law does not allow the processing of such data even with the subject's consent.

By way of derogation, data relating to political party affiliation, health status and receipt of social support may be processed without the consent of data subjects, insofar as this is allowed under the law.

In cases referred to in paragraphs 1 and 2 of this Article, processing must be specially labeled and protected by safeguards.

In cases referred to in paragraphs 1 and 2 of this Article, the Commissioner shall be entitled to access and ascertain the legality of data protection, wither *ex officio* or upon request of the data subject or controller.

The filing method and the safeguards applied to data referred to in paragraphs 1 and 2 of this Article shall be defined by the Government, upon obtaining the Commissioner's opinion.

Consent to Processing of Particularly Sensitive Data

Article 17

Consent to processing of particularly sensitive shall be given in writing and shall contain a designation of the data processed, the purpose of processing and the manner of use of such consent.

If a person giving consent is illiterate or otherwise incapable of signing the consent in hand, such consent shall be valid if two witnesses confirm by their signatures that the document represents the true intent of the person giving the consent.

Withdrawal of Consent to Processing of Particularly Sensitive Data

Article 18

In case of withdrawal, the person who previously gave his/her consent shall reimburse the controller for any and all justifiable costs incurred and damage sustained, in accordance with the regulations pertaining to damage liability, save where otherwise defined in the statement of consent.

Article 11 of this Law shall apply *mutatis mutandis* to withdrawals of consent to processing of particularly sensitive data.

III. RIGHTS OF DATA SUBJECTS AND PROTECTION OF RIGHTS OF DATA SUBJECTS

1. Rights

Right to Notification of Data Processing

Article 19

Data subjects shall have the right to be accurately and fully informed by the controller of the following:

1) Whether the controller is processing data on them and, if so, which processing operations it is performing;
2) Which data are being processed;
3) Who the data was collected from, i.e. who was the source of data;
4) The purposes for which the data is being processed;
5) The legal grounds for data processing;
6) Which data files contain the data;
7) Who uses such data;
8) Data and/or types of data that are used;

9) The purpose for which such data is used;

10) The legal grounds for the use of data;

11) Who receives the data;

12) Which data are transferred;

13) The purposes for which the data are transferred;

14) The legal grounds for data transfer;

15) The period in which the data are processed.

Right of Access

Article 20

Data subject shall have the right to request from controllers to access data relating to them.

The right of access to data relating to oneself shall include the right to review, read and listen to data, as well as the right to make notes.

Right to a Copy

Article 21

Data subjects shall have the right to request from controllers to obtain copies of data relating to them.

Controllers shall issue data copies (photocopies, audio-copies, video-copies, digital copies etc.) in the form in which such information is stored or in another form if such information would not be understandable to the data subject concerned if it were disclosed in the form in which it is stored.

Data subjects shall bear the necessary costs of making and providing copies of data.

Rights of Data Subjects upon obtaining Access to Data

Article 22

Data subjects shall have the right to require of controllers to correct, modify, update or delete data, as well as to a stay and suspension of processing.

Data subjects shall have the right to have their data deleted in the following cases:

1) If the purpose of processing is not clearly specified;

2) If the purpose of processing is changed, but the processing requirements for such changed purpose are not met;

3) If the purpose of processing has been achieved, i.e. if data is no longer needed for such purpose;

4) If data are processed by inadmissible means;

5) If data are such that their number or type is disproportionate to the purpose of processing;

6) If data are inaccurate and cannot be replaced with accurate ones by means of corrections;

7) If data are processed without consent or authority based on the law, as well as in other cases where processing is not allowed under this Law.

Data subjects shall have the right to have data processing stayed or suspended if they challenged the correctness, completeness and accuracy of data, as well as the right to have such data labeled as challenged pending a decision on their correctness, completeness and accuracy.

2. Restrictions

Restrictions of Rights

Article 23

The right to notification, access and copy may be restricted in the following cases:

1) If a data subject requests information referred to in Article 19, items 2) and 7) to 10) of this Law and the collector has already entered the data on him/her in a public register or has otherwise made them publicly available;

2) If a data subject abuses his/her right to notification, access and copy;

3) If the controller or another person has already notified to the data subject in accordance with Article 15 of this Law the information he/she requires, i.e. if the data subject has already accessed the information or obtained a copy and the data have not changed in the meantime;

4) If the controller would be prevented from performing duties within his sphere of competence;

5) If the provision of such information would significantly prejudice the interests of national or public safety, national defence or crime prevention, detection, investigation and prosecution;

6) If the provision of such information would significantly prejudice a major economic or financial interest of the state;

7) If the provision of such information would disclose data identified as confidential under a law or other regulations or enactment based on a law, insofar as the disclosure of such data could seriously prejudice an interest protected by the law;

8) If the provision of such information would seriously prejudice privacy or a vital interest of the data subject, in particular his/her life, health and physical integrity;

9) If data on the data subject are used solely for research and development purposes and statistical purposes, for as long as such usage of data continues.

Data subjects shall not have the right to access data during the stay of processing if the processing was stayed on their request.

3. Request

Request for Exercise of a Right

Article 24

Requests for notification, access and copy shall be submitted to controllers in writing, but controllers may also accept verbal requests for reasons of efficiency and cost-effectiveness. Requests for exercising one's rights upon obtaining access to data shall be submitted to controllers in writing.

Requests referred to in paragraph 1 of this Article shall contain: information on identity of the person filing the request (name and surname, name of one parent, date and town/city of birth, unique personal identification number); residence or dwelling address; as well as any other necessary contact information.

Requests filed by legal heirs of deceased persons shall also contain information on identity of such deceased persons. Enclosed with such requests, requesters shall submit death certificate and evidence of the requester's kinship with the deceased person.

Illiterate persons or persons unable to file requests in writing due to physical or other disabilities may make their requests verbally for the record.

Controllers may specify a format in which requests are to be filed, but they shall be required to take into consideration also any requests that are not made in such format.

If a request is unintelligible or incomplete, the controller shall instruct the requester to rectify any shortcomings.

If a requester fails to rectify shortcomings within the period specified, and in any case not later than 15 days of receipt of instruction to supplement a request, and if the shortcomings are such that the request cannot be processed, the controller shall dismiss such request as unacceptable by passing a relevant resolution.

4. Decision-making

Deciding on Requests for Notification, Access and Copy

Article 25

Controllers shall issue notices of filed requests without delay, and in any case not later than 15 days of the date of filing. Notices shall be issued in writing and, by way of exception, also verbally, if the requester agrees.

Controllers shall forthwith, and in any case not later than 30 days of receipt of an orderly request for access or obtaining a copy, enable the requester to access information or provide a copy of such information, as the case may be.

Together with the notice of granting access to data or of issuing copies of data, controllers shall also inform the requesters of the time, place and manner in which access to data will be enabled and the amount of necessary costs for producing copies of data and, if they do not have technical means at their disposal to issue a copy, they shall inform the requesters of the possibility to use their own equipment to make copies.

Requesters referred to in paragraph 2 of this Article may ask to access data at a time other than specified, where justifiable reasons for this pertain. As a rule, data shall be accessed on the controller's official premises.

If justifiable reasons prevent controllers from acting upon a request within the time limit set out herein, they shall notify the requester accordingly and set a new time limit for request processing, which time limit cannot be longer than 30 days of expiry of the rime limit referred to in paragraphs 1 and 2 of this Article.

If a controller accepts a request for notification, access and copy, he shall make a note thereon.

If a controller rejects a request, he shall pass a resolution thereon, with an instruction on available remedies.

If a controller fails to respond to a request within the time limits set out in paragraphs 1 and 2 of this Article, or if a controller rejects a request, the requester may appeal to the Commissioner.

Deciding on Requests upon Obtaining Access to Data

Article 26

Controllers shall decide on requests field upon obtaining access to data referred to in Article 24 of this Law without delay, and in any case not later than 15 days of the date of filing, and shall notify the requesters of their decisions accordingly.

If a controller rejects a request referred to in paragraph 1 of this Article, the rationale of the ruling shall specify the reasons for rejection, as well as the reasons why processing is allowed.

A requester may lodge an appeal with the Commissioner against a ruling on rejection of request referred to in paragraph 1 of this Article within 15 days of receipt of such ruling.

If a controller finds that a request filed upon obtaining access to data is grounded, but has no technical capacities for acting upon such request without delay or urgent action upon such request would require disproportionately high amounts of time or resources, such controller shall *ex officio* mark such data as challenged and temporarily stay their processing.

If a controller that is a public authority establishes that a request filed upon obtaining access to data is grounded, it shall mark such data as challenged and temporarily stay their processing. Such controller shall not modify, amend, update or delete data or suspend processing if:

1) The time limit for mandatory data retaining has not expired;

2) Acting upon a request would manifestly be seriously prejudicial to the interests of other persons;

3) Because of a special method of data storage, acting upon a request is impossible or would require disproportionately high amounts of time or resources.

A mark indicating data as challenged under Article 22, paragraph 3 of this Law shall be deleted pursuant to a decision of a competent authority or with the consent of the person to whom such data relate.

5. Methods of Exercising Rights

Method of Exercising the Right of Access

Article 27

Controllers shall make data relating to data subjects available to such data subjects in a comprehensible form.

Controllers shall make all data available to requesters in the given state.

If data are kept in different formats (paper, audio, video or electronic record etc.), requesters shall be entitled to access data in the format of their choice, except where this is impracticable.

Any person who is incapable of accessing data without a guardian may do so with the help of a guardian.

Upon request from persons who need specialist assistance to understand the content of data relating to them, controllers shall provide such assistance.

Controllers shall not subject the exercise of the right to access data to any fees.

Where a controller has at its disposal data in the language in which a request is made, it shall make the data available to the requester and produce a copy in such language, except where the requester specifies otherwise and the controller has the necessary capacities to comply with the request.

Methods of Exercising the Right to Copy

Article 28

Controllers shall issue copies of data (photocopy, audio copy, video copy, digital copy etc.) in the format in which such data are stored or in another format if data would be unintelligible to the requester in the format in which they are stored.

Requester shall bear the necessary costs of making and providing copies of data.

6. Processing for the Purposes of Public Media

Article 29

Processing by journalists and other media workers for the sole purpose of publication by mass media, with the exception of processing for advertising purposes, shall be governed by the provisions of Articles 3, 5 and 8(1) to (5) and Articles 46 and 47 of this Law.

Data relating to affiliation of persons with political parties may be used for the purposes of processing referred to in paragraph 1 of this Article, insofar as such data are relevant taking into account the public office held by the person concerned.

Attachment of Replies and Other Information

Article 30

Controllers shall attach any replies, corrections, retractions or any other information published on request from a data subject referred to in Article 29 of this

Law to the processed data and shall retain all such information for as long as the relevant data are kept.

Protection of Personality

Article 31

If the publication of data in mass media or in print constitutes a violation of a right or a legally protected interest of a person, the injured party may require the editor-in-chief and the publisher of a medium to notify him/her of the data processed about him/her, to grant him/her access to such data and to obtain a copy of such data, unless:

1) Such action would disclose data in connection with a data source which a journalist or another media worker is not required or willing to give;

2) Such action would disclose data in connection with a person who took part in the preparation and publication of such information and the editor-in-chief is not willing to disclose such data;

3) Circumstances pertain in which notification, accessing or issuing copies of data would significantly hamper the provision of information of public importance to the general public.

7. Special Provisions

Forwarding of Requests to the Commissioner

Article 32

If controllers are not processing the pertinent data, they shall forward requests to the Commissioner, save where the requester objects to such action.

Handling by the Commissioner

Article 33

Upon receipt of a request, the Commissioner shall establish whether a controller is processing the requested data.

If the Commissioner finds that a controller is not processing the data, he/she shall forward the request to the controller that is actually processing the data and shall notify the requester accordingly or shall instruct the requester to address the controller that is processing the data, as appropriate, taking into account the need to ensure that the request is handled in the most efficient way possible.

If the Commissioner finds that a controller is processing the data, he/she shall pass a ruling ordering such controller to decide on the request.

Controllers shall decide on requests referred to in paragraph 2 of this Article within the time limits set out in Article 25, paragraph 1, and Article 26, paragraph 1 of this Law from the date of submission, while decisions on requests referred to in paragraph 3 of this Article shall be made within seven days of service of the Commissioner’s ruling.

Proxy

Article 34

The rights enshrined in this Law may be exercised in person or through proxies.

A proxy must have a notarized power of attorney.

Retention and Use in the Event of Death

Article 35

In the event of death or if a missing person is declared dead, data collected under a contract or on the basis of consent given in writing shall be retained in accordance with the conditions set out in the contract or consent, while data collected pursuant to the law shall be retained for at least a year of the date of death or the data on which a missing person is declared dead, after which they shall be destroyed. An official notice shall be made of any destruction of data.

Consent for the use of data on deceased persons shall be given by the persons referred to in Article 10, paragraph 6 of this Law.

Controllers' Duties

Article 36

If a data file is formed under a contract or on the basis of consent in writing and such contract is terminated or such consent in writing is withdrawn, the controller shall delete the data within 15 days of contract termination or withdrawal of consent, unless provided for or agreed otherwise.

Application of Provisions of the Law on Administrative Proceedings *mutatis mutandis*

Article 37

The provisions of the law governing general administrative proceedings shall apply *mutatis mutandis* to the procedure of deciding upon requests, unless provided otherwise in this Law.

IV. APPEAL PROCEDURE

Right of Appeal

Article 38

Persons filing requests for exercising a right related to processing may lodge appeals with the Commissioner:

1) Against a controller's decision rejecting or denying a request;

2) If a controller fails to decide on a request within the specified time limit;

3) If a controller fails to grant access to data or issue a copy thereof or fails to do so within the time limit and in the manner provided for in this Law;

4) If a controller makes the issuing of a copy of data subject to the payment of a fee the amount of which exceeds the necessary costs of producing a copy;

5) If a controller, in violation of the Law, hampers or prevents the exercise of rights.

Appeals may be lodged within 15 days of the date of service of a decision rejecting or denying a request or upon expiry of the specified time limit for deciding and handling.

Enclosed with an appeal, requesters shall submit the relevant request with evidence of delivery to the controller and the challenged decision.

Handling of Appeals by the Commissioner

Article 39

The Commissioner shall decide on appeals within 30 days of lodging at the latest. Appeals shall be forwarded to the controller for reply. The appellant may file a rejoinder to the contestations stated in the appeal.

The Commissioner shall reject by means of resolutions all untimely or incomplete appeals or appeals lodged by unauthorized persons.

If the Commissioner, acting on an appeal lodged for failure to act upon request, establishes that the appeal is grounded, he/she shall order the controller to act upon request within a specified period of time.

If the controller, after the lodging of an appeal for failure to act upon request, but before the Commissioner rules on such appeal, enables the exercise of the right to access data or obtain a copy or if decides upon such request, the Commissioner shall terminate appeal proceedings by a resolution.

Appeal proceedings shall also be terminated if the appellant waives the appeal.

Establishment of Facts in Appeal Proceedings

Article 40

The Commissioner shall take such actions to establish the facts as may be necessary in order to rule on an appeal.

The Commissioner or a person specifically authorized by the Commissioner shall be given access to data or data files for the purpose of establishing the facts, except in cases referred to in Article 45, paragraph 2 of this Law.

Mandatory Nature and Enforcement of Rulings

Article 41

The Commissioner’s rulings on appeals shall be binding, final and enforceable.

Where necessary, the Government shall ensure that the Commissioner's rulings are enforced and may regulate in more detail the manner in which such rulings are to be enforced.

Legal Remedies against Rulings

Article 42

The Commissioner's rulings may be challenged in administrative proceedings.

Other Procedural Provisions

Article 43

The procedure of ruling on an appeal shall be governed by the law on general administrative proceedings, unless provided otherwise in this Law.

V. COMMISSIONER

Competences

Article 44

The Commissioner shall:

1) Supervise the enforcement of data protection;

2) Decide on appeals in cases set out in this Law;

3) Maintain the Central Register;

4) Supervise and allow transborder transfer of data from the Republic of Serbia;

5) Point out the identified cases of abuse in data collection;

6) Produce a list of countries and international organizations with adequate provisions on data protection;

7) Give his/her opinion on the formation of new data files or introduction of new information technologies in data processing;

8) Give his/her opinion in case of doubt whether a data set constitutes a data file within the meaning of this Law;

9) Give his/her opinion to the Government in the procedure of enactment of instruments governing the methods of data filing and safeguards for particularly sensitive data;

10) Monitor the implementation of data safeguards and suggests improvements;

11) Give proposals and recommendations for improving data protection;

12) Give prior opinion on whether a certain processing method constitutes specific risk for a citizen's rights and freedoms;

13) Keep up to date with the data protection arrangements in other countries;

14) Cooperate with authorities responsible for data protection supervision in other countries;

15) Determine the way in which data are to be handled if a data controller ceased to exist, unless provided otherwise;

16) Perform other duties within his/her sphere of competence.

The Commissioner may have a deputy responsible for personal data protection.

The Commissioner shall forward the report he/she submits to the National Assembly to the President of the Republic, the Government and the Ombudsperson and shall make it available to the general public through appropriate means.

Right of Access and Examination

Article 45

The Commissioner shall have the right of access to and examination of:

1) Data and data files;

2) Complete set of documents relating to data collection and other processing activities, as well as to the exercise of data subjects' rights under this Law;

3) General enactments of controllers;

4) Premises and equipment used by controllers.

The right of access and examination referred to in paragraph 1, items 1), 2) and 4) of this Article may be restricted if it could seriously prejudice the interests of national or public safety, national defence or crime prevention, detection, investigation and prosecution, for as long as reasons for such restrictions pertain in accordance with the law.

If a controller deems that reasons for restrictions referred to in paragraph 2 of this Article pertain, he shall, within eight days of service of a request, seek the opinion of the chairperson of the Supreme Court of Cassation to clarify whether reasons for restricting the Commissioner's right of access and examination pertain.

The chairperson of the Supreme Court of Cassation shall, within eight days of receipt of a request from a controller referred to in paragraph 3 of this Article, give his/her opinion to the controller. The controller shall notify the Commissioner of any such opinion of the chairperson of the Supreme Court of Cassation.

VI. DATA SECURITY

Confidentiality Duty

Article 46

The Commissioner, the Deputy Commissioner and the staff of the expert service shall keep the confidentiality of all data they learn during the performance of their duties, in accordance with the law and other regulations governing data confidentiality, unless provided otherwise.

The duty referred to in paragraph 1 of this Article shall subsist even after the Commissioner and the Deputy Commissioner have left office and after the staff of the expert service terminated their employment.

Controllers shall inform processors and persons who have access to data with the data confidentiality safeguards.

Organizational and Technical Measures

Article 47

Data must be adequately protected from abuse, destruction, loss, unauthorized alterations or access.

Controllers and processors shall take all necessary technical, human resources and organizational measures to protect data in accordance with the established standards and procedures in order to protect data from loss, damage, inadmissible access, modification, publication and any other abuse, as well as to provide for an obligation of keeping data confidentiality for all persons who work on data processing.

VII. RECORDS

Data Processing Records

Article 48

Controllers shall establish and maintain records containing the following information:

1) Type of data and name of data file;
2) Type of processing activities;
3) Business name, name, head office and address of the controller;
4) Date of commencement of data processing or date of data file creation;
5) The purpose of processing;
6) The legal grounds for data processing or creation of data file;
7) The category of data subjects;
8) The type and degree of data confidentiality;
9) The method of data collection and keeping;
10) The time limit for data keeping and use;
11) Business name, name, head office and address of the data user;
12) The mark under which data are transferred in or out of the Republic of Serbia, with an indication of the state or international organization and the foreign data user, the legal grounds and the purpose of transborder transfer in or out of the country;
13) Safeguards put in place to protect data;
14) Requests concerning data processing.

Controllers shall not be required to set up and maintain records for the processing of: data collected solely for family purposes and other personal purposes within the meaning of Article 5, item 2) of this Law; data processed for the purpose of maintaining registers required by the law; data in data files that contain only publicly available data; and data relating to persons whose identity remains undisclosed and the controller, the processor or the user is not authorized to establish such person's identity.

Controllers shall update the records whenever a change occurs in relation to the basic data referred to in paragraph 1 of this Article within 15 days of the date when such change occurs.

The format of records and the manner of keeping of records referred to in paragraph 1 of this Article shall be specified by the Government.

Notification of the Commissioner

Article 49

Before the commencement of data processing or creation of data files, as the case may be, controllers shall notify the Commissioner of their intent to form a data file, with enclosed data referred to in Article 48 of this Law, as well as of any intended subsequent processing, such notification being due before the processing takes place and in any case not later than 15 days before the formation of the data file or before data processing.

The notification duty set out in paragraph 1 of this Article shall not apply to the commencement of data processing or creation of data files in cases where special regulations govern the purpose of processing, the type of data processed, the categories of users with access to the data and the period during which such data will be retained.

Prior Verification

Article 50

Upon receipt of a notification referred to in Article 49 of this Law and before the formation of a data file, the Commissioner shall verify any processing activities that could significantly prejudice the rights of data subjects.

The method in which verifications referred to in paragraph 1 of this Article are to be carried out shall be specified in an enactment passed by the Commissioner.

Duty to Submit

Article 51

Controllers shall submit to the Commissioner records of data files or changes in data records at the latest within 15 days of the date of data file formation or change.

The notifications referred to in Article 49, paragraph 1 of this Law and the records referred to in paragraph 1 of this Article shall be entered in the Central Register.

Central Register

Article 52

The Commissioner shall form and maintain the Central Register.

The Central Register shall comprise a register of data files and a catalogue of data files.

The register of data files shall contain the data referred to in Article 51, paragraph 2 of this Law.

The catalogue of data files shall contain a description of recorded data files.

The Central Register shall be public and has to be published on the Internet.

The Commissioner shall once a year publish an inventory of data files in the "Official Gazette of the Republic of Serbia".

The Commissioner shall deny access to the record of data files upon request of a data controller, provided this is necessary for the achievement of a prevailing interest of national or public safety, national defence, crime prevention, detection, investigation and prosecution, or economic or financial interests of the state, or if a law or another regulation or enactment adopted pursuant to a law provide for the confidentiality of the record of data files.

VIII. TRANSBORDER TRANSFER OF DATA OUT OF THE REPUBLIC OF SERBIA

Article 53

Data can be transferred from the Republic of Serbia to a state party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Data may be transferred from the Republic of Serbia to a state that is not a party to the Convention referred to in paragraph 1 of this Article or an international organization if such state or international organization has a regulation or a data transfer agreement in force which provides a level of data protection equivalent to that envisaged by the Convention.

In cases of transborder transfer of data referred to in paragraph 2 of this Article, the Commissioner shall determine whether the requirements are met and safeguards put in place for the transfer of data from the Republic of Serbia and shall authorize such transfer.

IX. SUPERVISION

Competence

Article 54

The implementation of and compliance with this Law shall be supervised by the Commissioner.

The Commissioner shall perform the duties referred to in paragraph 1 of this Article through authorized officers.

Authorized officers shall carry out their supervision duties in a professional and timely fashion and shall produce records of their enforcement activities.

In supervising the enforcement of the Law, authorized officers shall use knowledge acquired *ex officio* or learned from appellants or third parties.

In supervising the enforcement of the Law, authorized officers shall furnish their official identification documents. The format of such identification documents shall be prescribed by the Commissioner.

Facilitation of Supervision

Article 55

Persons responsible for data protection under this Law shall enable authorized officers to freely carry out supervision duties and shall give them access to all necessary documents.

Commissioner's Supervision Powers

Article 56

If violations of the provisions of this Law pertaining to processing are identified in the course of supervision, the Commissioner shall caution the controller against any irregularities in processing.

On the basis of the findings of an authorized officer, the Commissioner may:

1) Order the rectification of such irregularities within a specified period of time;

2) Temporarily ban any processing carried out contrary to the provisions of this Law;

3) Order the deletion of data collected without proper legal grounds.

Orders referred to in paragraph 2 of this Article shall not be subject to appeal, but they may be challenged in administrative proceedings.

The implementation of measures referred to in paragraph 2 of this Article shall be governed by an enactment of the Commissioner.

The Commissioner shall *ex officio* file petitions for institution of infringement proceedings in cases of violation of the provisions of this Law.

X. PENAL PROVISIONS

Article 57

A fine in the amount of RSD 50,000 to 1,000,000 shall be charged for infringement to a collector, a processor or a user with the status of a legal entity that:

1) Processes data without consent, contrary to the provisions of Article 12 of this Law;

2) Processes data contrary to the provisions of Article 13 of this Law;

3) Collects data from a third party contrary to the provisions of Article 14, paragraph 2 of this Law;

4) Before the collection of data, fails to inform the data subject or a third party of the requirements of Article 15, paragraph 1 of this Law;

5) Processes particularly sensitive data contrary to the provisions of Articles 16 to 18 of this Law;

6) Fails to make all data available in their current format, contrary to Article 27, paragraph 2 of this Law;

7) Fails to issue a copy of data in the current format, contrary to Article 28, paragraph 1 of this Law;

8) Fails to delete data from a data file contrary to Article 36 of this Law;

9) Fails to proceed in accordance with the Commissioner's ruling on appeal (Article 41, paragraph 1 of this Law);

10) Acts in violation of the confidentiality duty referred to in Article 46, paragraphs 1 and 2 of this Law;

11) Acts in violation of the duty to take the measures referred to in Article 47, paragraph 2 of this Law;

12) Fails to form or update a record in violation of Article 48, paragraphs 1 and 3 of this Law;

13) Fails to notify the Commissioner of its intent to form a data file within the specified period of time, contrary to Article 49, paragraph 1 of this Law;

14) Fails to submit to the Commissioner its record of data files or changes in data files within the specified period of time (Article 51, paragraph 1 of this Law);

15) Transfers data from the Republic of Serbia contrary to Article 53 of this Law;

16) Fails to enable an authorized officer to freely perform supervision activities and grant him/her access to all necessary documents (Article 55 of this Law);

17) Fails to act on the Commissioner's orders (Article 56, paragraph 2 of this Law).

For infractions referred to in paragraph 1 of this Article, an entrepreneur shall be charged a fine in the amount of RSD 20,000 to 500,000.

For infractions referred to in paragraph 1 of this Article, a natural person or the responsible officer of a legal entity, public authority, body or territorial autonomy and local self-government unit shall be charged a fine in the amount of RSD 5,000 to 50,000.

XI. TRANSITIONAL AND FINAL PROVISIONS

Article 58

The head office, appointment, termination of office, procedure for relieving of duty, the status of the Commissioner, the Deputy Commissioner and the expert service, funding and reporting shall be governed by the provisions of the Law on Free Access to Information of Public Importance ("Official Gazette of the Republic of Serbia" Nos. 120/04 and 54/07).

Article 59

The Commissioner for Information of Public Importance, established under the Law on Free Access to Information of Public Importance ("Official Gazette of the Republic of Serbia" Nos. 120/04 and 54/07) shall continue to operate as the Commissioner for Information of Public Importance and Personal Data Protection.

Article 60

Secondary legislation hereunder shall be passed within six months of the date when this Law comes into force.

Article 61

Data files and records formed by the date when this Law comes into force shall be harmonized with the provisions hereof within 12 months of the date when this Law comes into force.

Data controllers shall submit the records referred to in Article 48 of this Law to the Commissioner within 12 months of the date when this Law comes into force.

Article 62

As of the date when this Law comes into force, the Personal Data Protection Law ("Official Gazette of FRY" No. 24/98 and 26/98-Corrigendum) shall be superseded and extinguished.

Article 63

This Law shall come into force on the eighth day of its publication in the "Official Gazette of the Republic of Serbia" and shall take effect as of 1 January 2009.