

DRAFT LAW ON PERSONAL DATA PROTECTION

I. BASIC PROVISIONS

Subject matter of the Law

Article 1.

This law regulates the right to protection of the data subjects in relation to personal data processing and free flow of this data, principles of processing, the rights of the data subjects, the obligations of controllers and processors, code of conduct, certification transfer of personal data to other countries and international organizations, monitoring over the implementation of this law, legal remedies, accountability and sanctions in case of breach of the rights of natural persons in relation to personal data processing, as well as specific cases of processing.

This law regulates, in particular, the protection of rights of natural persons in relation to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the prevention and protection of threats to public and national security as well as free flow of such data.

Objectives of the Law

Article 2.

This law ensures respect of fundamental rights and freedoms of natural persons, and in particular their right to protection of personal data.

The provisions of special laws governing personal data protection must be in line with this Law.

Scope of application

Article 3.

This Law applies to the processing of personal data wholly or partly by automated means and to the processing of personal data other than by automated means which form a part of a filing system or are intended to form a part of a filing system.

This Law does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.

This Law applies to the processing of personal data performed by a controller or a processor, with business seat, permanent or temporary residence in the territory of the Republic of Serbia, in the framework of activities undertaken in the territory of the Republic of Serbia regardless of whether the processing takes place in the territory of the Republic of Serbia or not.

This Law applies to the processing of personal data of data subjects who have a permanent or temporary residence in the territory of the Republic of Serbia by a controller or processor who is not established or does not have permanent or temporary residence in the territory of the Republic of Serbia, if the processing activities are related to:

a) the offering of goods or services to the data subject in the territory of the Republic of Serbia, irrespective of whether a payment is required for these goods or services,

b) the monitoring of activities of the data subject if they take place within the territory of the Republic of Serbia.

Definitions

Article 4.

Specific terms in this law have the following meaning:

1) 'personal data' means any information relating to a natural person identified or identifiable, directly or indirectly, in particular by reference to his/her identity, such as name and an identification number, location data, an online identifier, or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity;

2) "data subject" means a natural person whose personal data are processed;

3) 'processing of personal data' ('processing') means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, combination or structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or submission, multiplication, dissemination or otherwise making available, alignment, restriction, erasure or destruction;

4) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

5) 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate or predict certain personal aspects relating to a natural person, in particular concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

6) 'pseudonymisation' means the processing of personal data in such manner that prevents the personal data to be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures that ensure that the personal data cannot be attributed to an identified or identifiable natural person;

7) 'filing system' means any structured set of personal data accessible according to specific criteria, whether the filing system is centralised, decentralised or dispersed on a functional or geographical basis;

8) 'controller' means the natural or legal person, public authority body, which, alone or jointly with others, determines the purposes and means of the processing of personal data; The law establishing the purposes and means of processing may determine the controller or prescribe the conditions for its designation;

9) 'processor' means a natural or legal person, public authority body which processes personal data on behalf of the controller;

10) 'recipient' means a natural or legal person, or public authority body, to which the personal data are disclosed, whether a third party or not, except if these are public authority

bodies which may receive personal data in the framework of a particular inquiry in line with law and the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

11) 'third party' means a natural or legal person, public or authority body other than the data subject, controller, processor or persons who, under the direct authority of the controller or processor, are authorised to process personal data;

12) 'consent' means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

13) 'personal data breach' means a breach of security of personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

14) 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person, and in particular those obtained from an analysis of a biological sample;

15) 'biometric data' means personal data resulting from specific technical processing and relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

16) 'data concerning health' means information related to the physical or mental health of a natural person, including the data on the provision of health care services, which reveal information about his or her health status;

17) 'representative' means a natural or legal person with a place of residence or headquarters within the territory of the Republic of Serbia who is designated, in line with Article 44 of this Law, to represent the controller or processor with regard to their respective obligations under this Law;

18) 'enterprise' means a natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly engaged in an economic activity;

19) 'multinational company' means a business entity that is the controlling founder or controlling member of an undertaking or founder of a branch of an undertaking engaged in an economic activity in a country in which its seat is not located, as well as a business entity with significant participation in a business entity or in a founder of a branch of a business entity, performing an economic activity in a country where the seat of a multinational company is not located, in accordance with the law governing enterprises;

20) 'group of undertakings' means a group of joined enterprises pursuant to law governing joined enterprises;

21) 'binding corporate rules' means personal data protection internal policies which are adhered to and implemented by a controller or processor, established on the territory of the Republic of Serbia for the purpose of regulating the transfers of personal data to a controller or processor in one or more countries within the multinational company or group of undertakings;

22) 'Commissioner for information of public importance and personal data protection (hereinafter: the Commissioner) means an independent and autonomous public authority body established by law, which is competent for the supervision over the implementation of this law and performs other tasks pursuant to law;

23) 'information society service' means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services;

24) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

25) 'public authority' means a public authority body, a territorial autonomy body and a local self-government unit, a public enterprise, institution and other public service, an organization and other legal or natural person performing public authority;

26) ‘competent authorities’ are:

- a) public authority bodies competent for the prevention, investigation and detection of criminal offences and prosecution of offenders or the execution of criminal penalties, including the prevention and protection from threats to public and national security;
- b) a legal person authorized by law to perform the tasks referred to in sub-item 1) of this Item.

II. PRINCIPLES

Principles of personal data processing

Article 5.

Personal data shall be:

- 1) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’). Lawful processing is processing performed in line with this or other law governing personal data protection.
- 2) collected for specified, explicit, justified and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’);
- 3) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- 4) accurate and, where necessary, kept up to date; having regard to the purposes for which they are processed, every reasonable measure must be taken to ensure that inaccurate personal data are erased or rectified without delay (‘accuracy’);
- 5) kept in a form which permits identification of data subject for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’);
- 6) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by implementation of appropriate organizational, staffing or technical protection measures (‘integrity and confidentiality’)

The controller shall be responsible for the implementation of the principles referred to in para 1 of this Article; the controller must be able to demonstrate compliance with the principles referred to in para 1 of this Article; ('accountability').

Other purposes of processing

Article 6.

Exceptionally from Article 5 Para 1 Item 2 of this Law, if further processing of personal data is carried out for the purpose of archiving in the public interest, scientific or historical research, as well as for statistical purposes, in accordance with this Law, it shall be considered that processing of personal data is not performed in a way that is not in line with the original purpose.

If personal data processing , intended to be performed for purposes different from the one for which the data were collected, is not based on the law which prescribes necessary and proportionate measures in a democratic society to safeguard the objectives referred to in Article 40 Para 1 of this Law, or the consent of the data subject, the controller shall assess whether that other purpose of processing is in accordance with the processing purpose for which the data was collected, taking into account in particular:

- 1) whether there is a connection between the purpose for which the data were collected and other purposes of the intended processing;
- 2) the circumstances in which the data were collected, including the relationship between the controller and the data subject;
- 3) the nature of the data, and in particular whether special types of personal data referred to in Article 17 of this Law is processed, namely the personal data on the criminal judgments and criminal offences referred to in Article 19 of this Law;
- 4) possible consequences of further processing for the data subject;
- 5) the application of appropriate measures, such as cryptographic protection and pseudonymization.

Provisions of the Paras 1 and 2 of this Article shall not apply to the processing of personal data by competent authorities by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public and national security (hereinafter: special purposes of processing).

Other purpose of processing by competent authorities

Article 7.

Personal data collected by the competent authorities for other purposes cannot be processed for the purpose that is different than the purpose for which the data were collected, unless that further processing is provided by law.

Personal data processing by the competent authorities for other purposes, which are different from the purpose for which the data were collected, is permitted if the following conditions are fulfilled jointly:

1) the controller is authorized to process these data for that other purpose, in accordance with the law;

2) processing is necessary and proportional to that other purpose, in accordance with the law.

Personal data processing by the competent authorities for other purposes may include the archiving of personal data in the public interest, or their use for scientific, statistical or historical purposes, provided that appropriate organizational, staffing and technical measures are applied in order to protect the rights and freedoms of the data subjects.

Storage, time limits for storage periods and review in specific cases

Article 8.

Exceptionally from Article 5 Para 1 Item 5 of this Law, personal data processed exclusively for the purposes of archiving in the public interest, scientific or historical

research, as well as for statistical purposes may be kept for a longer period, subject to the provisions of this Law on the application of appropriate organizational, staffing and technical measures aimed at protecting the rights and freedoms of the data subjects.

In the case of personal data processed by competent authorities for other purposes, appropriate time limits for the erasure of personal data or for a periodic review of the need for their storage shall be established.

The controller shall determine the time limit referred to in Paras 1 and 2 of this Article, if it is not determined by law.

The Commissioner shall monitor the compliance with the time limits referred to in Paras 1 to 3 of this Article in line with its competences prescribed by this Law.

Distinction between different categories of data subjects

Article 9.

In the case of personal data processed by competent authorities for special purposes, the competent authority shall, whenever possible, make a clear distinction during processing, between data relating to certain types of persons whose personal data is processed, such as:

- 1) persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence;
- 2) persons with regard to whom there is reasonable suspicion that they have committed a criminal offence;
- 3) persons convicted of a criminal offence;
- 4) victims of a criminal offence or persons with regard to whom there are reasons for believing that they could be the victim of a criminal offence; and
- 5) other parties to a criminal offence, such as witnesses, or persons who can provide information on criminal offences, other persons connected to them or associates of persons referred to in items 1 to 3 of this article.

Distinction between certain categories of personal data

Article 10.

When personal data is processed by competent authorities for special purposes, the competent authority shall, to the extent possible, provide for personal data based on facts to be clearly distinguished from personal data based on personal assessments.

Assessment of quality of personal data and specific conditions of processing by competent authorities for special purposes

Article 11.

The competent authorities processing personal data for special purposes shall take all reasonable steps to ensure that personal data which are inaccurate, incomplete or no longer up to date, are not transmitted or made available.

The competent authority shall verify, to the extent possible, whether personal data are accurate, complete or up to date, before they are transmitted or made available.

The competent authority transferring personal data to the competent authority, shall provide, to the extent possible, necessary information enabling the assessment of the degree of accuracy, completeness, verifiability or reliability of personal data, and the extent to which they are up to date.

If it emerges that incorrect personal data have been transmitted or personal data have been unlawfully transmitted to the competent authority, that authority shall be notified without delay and the personal data shall be rectified or erased or processing shall be restricted in accordance with this law.

If personal data processing requires the fulfilment of special conditions, the competent authority shall inform the recipient of these data of these special conditions and its obligation to fulfil them.

Lawfulness of processing

Article 12.

Processing shall be lawful, only if and to the extent to which, one of the following conditions is fulfilled:

1) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

2) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps prior to entering into a contract, at the request of the data subject;

3) processing is necessary in order to comply with legal obligations of the controller;

4) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

5) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6) processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of data subject, which requires protection of personal data, in particular when the data subject is a child.

Item 6 Para 1 of this Article shall not apply to processing carried out by public authority bodies in the performance of their tasks.

The provisions of Paras 1 and 2 of this Article shall not apply in case of data processing by competent authorities for special purposes.

Lawfulness of data processing by competent authorities for special purposes

Article 13.

Data processing by competent authorities for special purpose is lawful only if that processing is necessary for the performance of a task carried out by competent authorities laid down by law. Such a law specifies at least the objectives of processing, the personal data to be processed and the purposes of the processing.

Lawfulness of processing data in specific cases

Article 14.

The grounds for data processing referred to in Article 12 Para 1 Items 3) and 5) shall be determined by law.

In case of processing referred to in Article 12 Para 1, Item 3) of this Law, the law referred to in Para 1 of this Article shall determine the purpose of the processing, and in the case of processing referred to in Article 12, Para 1, Item 5) of this Law, the law referred to in Para 1 of this Article shall prescribe that processing is necessary in order to carry out the tasks in the public interest or exercise official authority vested in the controller by law.

The law referred to in Para 1 of this Article shall prescribe the public interest to be achieved, as well as the duty to respect the rules on proportionality of processing in relation to the aim to be achieved, and may also prescribe the conditions governing the lawfulness of processing by the controller, the types of data which are subject to the processing; the data subjects concerned, the persons to which the personal data may be disclosed, and the purposes of disclosure, the purpose limitation, storage periods, processing operations and processing procedures, and measures to ensure lawful and fair processing.

Consent

Article 15.

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

If the data subject's consent is given in the context of a written declaration of a person which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in comprehensible and easily accessible form, using clear and plain language. Any part of such a written declaration which constitutes an infringement of this Law shall not be binding.

The data subject shall have the right to withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of processing performed based on consent before the withdrawal. Prior to giving consent, the data subject shall be informed about the right to withdrawal of the consent and its effects. The withdrawal of consent shall be made as easy as giving consent.

When assessing whether consent for processing personal data is freely given, utmost account shall be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Consent of a minor in relation to the use of information society services

Article 16.

A 15 years old person may autonomously give consent for the processing of his or her personal data in relation to the offer of information society services.

For the processing of the personal data referred to in Para 1 of this Article, of a person who is below the age of 15, consent shall be given by a parent exercising parental rights or legally authorized holders of parental responsibility over the child.

The controller shall undertake reasonable measures to verify in such cases that the consent is given by parents or legally authorized holders of parental responsibility over the minor, taking into consideration available technology.

Processing of special categories of personal data

Article 17.

Processing of personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, shall be prohibited.

Exceptionally, data processing referred to in Para 1 of this Article shall be allowed in the following cases:

- 1) the data subject has given explicit consent to the processing of data referred to in Para 1 for one or more specified purposes, except where law provides that the processing of those data cannot be performed on the basis of consent;

- 2) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security and social protection, if processing is prescribed by law or a collective agreement, while providing for appropriate safeguards for the fundamental rights, freedoms and the interests of the data subject;
- 3) processing is necessary to protect the vital interests of the data subject or of another natural person, if the data subject is physically or legally incapable of giving consent due to the lack of legal capacity;
- 4) processing is carried out in the course of legitimate activities and providing for appropriate safeguards by endowment, foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim, under the condition that the processing relates solely to the members or former members of the organisation or to persons who have regular contact with it in connection with its purposes, and that the personal data shall not be disclosed outside of that organization without the consent of the data subject;
- 5) processing relates to personal data which are manifestly made public by the data subject;
- 6) processing is necessary for the establishment, exercise or defence of legal claims or whenever the courts are acting within their judicial capacity;
- 7) processing is necessary for reasons of substantial public interest, on the basis of law, if processing is proportionate to the aim pursued, respecting the essence of the right to data protection and if the law provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- 8) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems, on the basis of law or pursuant to contract with a health professional, under the condition that processing is performed by or under the supervision of a health professional or other person under the obligation of professional secrecy prescribed by law or professional rules;

- 9) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to public health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular regarding professional secrecy;
- 10) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with law and Article 92 Para 1 of this Law, if processing is proportionate to the aim pursued, respecting the essence of the right to data protection and if the law provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The provisions of Paras 1 and 2 of this Article shall not apply to data processing by competent authorities for special purposes.

Processing of specific categories of personal data by competent authorities for special purposes

Article 18.

Processing of personal data by competent authorities for special purposes, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and the processing of genetic data, biometric data, for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only in one of the following cases:

- 1) where competent authority is authorised by law to process specific categories of personal data;
- 2) processing of specific categories of data is performed to protect the vital interests of the data subject or of another natural person;

3) processing refers to specific categories of data which are manifestly made public by the data subject.

Processing of personal data relating to criminal records and criminal offences

Article 19.

Processing of personal data relating to criminal convictions, criminal offences and security measures may be performed based on Article 12 Para 1 of this Law, only under the control of official authority or when the processing is authorized by law, while providing for appropriate safeguards for the rights and freedoms of data subjects.

Any comprehensive register of criminal convictions shall be kept only by the official authority and under the control of official authority.

Processing which does not require identification

Article 20.

If the purposes of processing personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be required to acquire, process or maintain additional information in order to identify the data subject, only for the purpose of the implementation of this Law in relation to data processing.

Where, in cases referred to in Para 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible.

In case referred to in Paras 1 and 2 of this Article, the provisions of Articles 26 Paras 1 to 4, Article 29, Article 30 Paras 1 to 5, Article 31 Paras 1 to 3, Article 33 Paras 1 and 2 and Article 36 Paras 1 to 4 of this Law shall not apply, except if the data subject, for the purpose of exercising his or her rights under those Articles, provides additional information enabling his or her identification.

The provisions of Paras 2 and 3 of this Article shall not apply in case of data processing by competent authorities for special purposes.

III. RIGHTS OF THE DATA SUBJECT

1. TRANSPARENCY AND MODALITIES FOR THE EXERCISE OF THE RIGHTS

Transparent information, communication and modalities for the exercise of the rights of the data subject

Article 21.

The controller shall take appropriate measures to provide the data subject with any information referred to in Articles 23 and 24 of this Law and any information regarding the exercise of rights under Articles 26, Articles 29 to 31, Article 33 and Article 36 to 38 and in connection to Article 53 of this Law in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. This information shall be provided in writing, or by other means, including, where appropriate, by electronic means. If the data subject requires, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The controller shall facilitate the exercise of data subject rights under Articles 26, Articles 29 to 31, Article 33 and Articles 36 to 38 of this Law. In the cases to which Article 20 Paras 2 and 3 of this Law refer, the controller shall not refuse to act upon the request of the data subject for exercising his or her rights under Article 26, Articles 29 to 31, Article 33 and Articles 36 to 38 of this Law, unless the controller demonstrates that it is not in a position to identify the data subject.

The controller shall provide information on action taken upon a request under Article 26, Articles 29 to 31, Article 33 and Articles 36 to 38 of this Law to the data subject without undue delay and in any event within 30 days of receipt of the request. That period may be extended by additional 60 days where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within 30 days of the receipt of the request, along with the reasons for the delay. Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

If the controller does not take action upon the request of the data subject, the controller shall inform the data subject without delay and at the latest within 30 days of the receipt of the request of the reasons for not taking action and on the possibility of using legal remedy before the Commissioner or the court.

The controller shall provide information referred to in Articles 23 and 24 of this Law, or information related to the exercise of data subject rights under Article 26, Articles 29 to 31, Article 33 and Articles 36 to 38 and in connection to Article 53 of this Law free of charge. Where request by a data subject is manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

- 1) charge the necessary administrative costs of providing the information or taking the action requested; or
- 2) refuse to act upon the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Article 26, Articles 29 to 31, Article 33 and Articles 36 to 38 of this Law, the controller may request the provision of additional information necessary to confirm the identity of the data subject, without prejudice to implementation of Article 20 of this Law.

The information to be provided to data subjects pursuant to Articles 23 and 24 of this Law may be provided in combination with standardised icons presented in electronic form, in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the standardized icons are presented electronically, they shall be machine-readable.

The Commissioner shall determine the information to be provided in standardised icons presented in electronic form and the procedure for determining standardised icon.

Provisions referred to in Paras 1 to 9 of this Article shall not apply to the data processing by competent authorities for special purposes.

Communication and modalities for exercising the rights of the data subject in case of
processing by competent authorities for special purposes

Article 22.

Where personal data is processed by competent authorities for special purposes, the controller shall take reasonable steps to provide the data subject with any information referred to in Article 25 of this Law, or information related to exercising the rights referred to in Articles 27, 28, 32, 34, 35, 39 and Article 53 of this Law, in a concise, intelligible and easily accessible form, using clear and plain language. The information shall be provided by any appropriate means, including by electronic means. As a general rule, the controller shall provide the information in the same form as the request of the data subject.

The controller shall facilitate the data subject in the exercise of the rights under Articles 27, 28, 32, 34, 35, and Article 39 of this Law.

The controller shall inform the data subject in writing about the follow up to his or her request without undue delay.

The controller shall provide the information referred to in Article 25 of this Law and act in line with Articles 27, 28, 32, 34, 35, 39 and Article 53 of this Law free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the competent authority may either:

- 1) charge the necessary administrative costs of providing the information or taking the action requested; or
- 2) refuse to act on the request;

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Where the controller has reasonable doubts concerning the identity of the natural person making a request referred to in Article 27 or Article 32 of this Law, the controller may request the provision of additional information necessary to confirm the identity of that person.

2. INFORMATION AND ACCESS TO PERSONAL DATA

Information to be provided where personal data are collected from the data subject

Article 23.

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are collected, provide the data subject with the following information:

- 1) the identity and the contact details of the controller and of the controller's representative where applicable;
- 2) the contact details of the data protection officer, where applicable;
- 3) the purposes of the intended processing, as well as the legal basis for the processing;
- 4) the legitimate interests pursued by the controller or by a third party, where the processing is based on Article 12 Para 1 Item 6 of this Law;
- 5) the recipient, or categories of recipients of the personal data, if any;
- 6) the fact that the controller intends to transfer personal data to a third country or international organisation and whether that country or international organisation is on the list referred to in Article 64 Para 7 of this Law, and in the case of transfers referred to in Articles 65 and 67 or Article 69 Para 2 of this Law, about the reference to the appropriate safeguards and the means by which data subject can be acquainted with them.

In addition to the information referred to in Para 1 of this Article, the controller shall, at the time when personal data are collected, provide the data subject with the following further information that may be necessary to ensure fair and transparent processing, pending the circumstances of the case:

- 1) the period for which the personal data will be stored, or if it is not possible, the criteria used to determine that period;

2) the existence of the right to request from the controller access, rectification or erasure of personal data concerning the data subject or right to restriction of the processing or right to object to the processing, as well as the right to data portability;

3) where the processing is based on Article 12 Para 1 Item 1) of this Law, or Article 17 Para 2 Item 1) of this Law, of the existence of the right to withdraw consent at any time, and that withdrawal of consent shall not affect the lawfulness of processing based on the consent before its withdrawal;

4) the right to lodge a complaint with the Commissioner;

5) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data, and of the possible consequences of failure to provide such data;

6) the existence of automated decision-making, including profiling, referred to in Article 38 Paras 1 and 4 of this Law and at least in those cases meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where the controller intends to further process the personal data for a purpose other than the one for which the personal data were collected in line with this Law, the controller shall, prior to that further processing, provide the data subject with information on that other purpose and with any relevant further information, as referred to in Para 2 of this Article referring to that other purpose.

If the data subject already has some of the information referred to in Paras 1 to 3 of this Article, the controller shall not be obliged to provide that information.

Provisions referred to in Paras 1 to 4 of this Article shall not apply to the data processing by competent authorities for special purposes.

Information to be provided when personal data are not obtained from the data subject

Article 24.

Where personal data are not obtained from the data subject, the controller shall provide the data subject with the following information:

1) the identity and the contact details of the controller and, where applicable, of the controller's representative;

2) the contact details of the data protection officer, where applicable;

3) the purposes of the intended processing and the legal basis for the processing;

4) the categories of personal data processed;

5) the recipient or categories of recipients of the personal data, if any;

6) the fact that the controller intends to transfer personal data to a third country or international organization and whether that country or international organisation is on the list referred to in Article 64 Para 7 of this Law, and in the case of transfers referred to in Articles 65 and 67 or Article 69 Para 2 of this Law, about the reference to the appropriate or suitable safeguards and the means how data subject can be acquainted with them.

In addition to the information referred to in Para 1 of this Article, when obtaining personal data, the controller shall provide the data subject with the following information that may be necessary to ensure fair and transparent processing in respect of the data subject pending the circumstances of the case:

1) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

2) the legitimate interests pursued by the controller or by a third party, if the processing is performed on the basis of Article 12 Para 1 Item 6 of this Law;

3) the existence of the right to request from the controller access, rectification or erasure of personal data or right to restriction of the processing and right to object to the processing as well as the right to data portability;

4) where processing is based on Article 12 Para 1 Item 1 of this Law or Article 17 Para 2 Item 1 of this Law, about the existence of the right to withdraw consent at any time,

and that withdrawal of consent does not affect the lawfulness of processing based on the consent before its withdrawal;

5) the right to lodge a complaint with the Commissioner;

6) the source from which the personal data originate, and, where applicable, whether the data originate from publicly accessible sources;

7) the existence of automated decision-making including profiling, referred to in Article 38 Paras 1 and 4 of this Law and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The controller shall provide the information referred to in Paras 1 and 2 of this Article:

1) within a reasonable period after collecting the personal data, but at the latest within 30 days, having regard to all the circumstances in which the personal data are processed;

2) if the personal data are used for communication with the data subject, at the latest at the time of the first communication with the data subject;

3) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

If the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall, prior to that further processing, provide the data subject with information on that other purpose and with any relevant further information, as referred to in Para 2 of this Article.

The controller shall not be obliged to provide data subject with information referred to in Paras 1 to 4 of this Article if:

1) the data subject already has the information;

2) the provision of such information proves impossible or would involve a disproportionate amount of time and resources, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical

purposes, if the conditions and safeguards referred to in Article 92 Para 1 of this Law are applied or in so far as the obligation referred to in Para 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases, the controller shall take appropriate measures to protect the data subject's rights, freedoms and legitimate interests, including making the information referred to in Paras 1 to 4 of this Article publicly available;

3) collection or disclosure of personal data is expressly laid down by law which provides appropriate measures to protect the data subject's legitimate interests ;

4) where the personal data must remain confidential subject to legally prescribed obligation of professional secrecy.

Provisions referred to in Paras 1 to 5 of this Article shall not apply to the data processing by competent authorities for special purposes.

Information to be made available or given to the data subject in case of data processing by competent authorities for special purposes

Article 25.

Where information is processed by competent authority for special purposes, the controller shall make available to the data subject at least the following information:

- 1) the identity and the contact details of the controller;
- 2) the contact details of the data protection officer, if it exists;
- 3) the purposes of the intended processing;
- 4) the right to lodge a complaint with the Commissioner and contact details of the Commissioner;
- 5) the existence of the right to request from the controller access, rectification or erasure of personal data relating to him/her and restriction of processing.

In addition to the information referred to in Para 1 of this Article, the controller shall give to the data subject, the following further information, to enable the exercise of his or her rights, pending the specific circumstances of the case:

- 1) the legal basis for the processing;

2) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;

3) the categories of recipients of the personal data, if they exist, including in third countries or international organisations;

4) further information, where necessary, in particular where the personal data are collected without the knowledge of the data subject.

Provision of information referred to in Para 2 of this Article to the data subject, which refer to certain categories of processing, may be restricted, omitted or delayed only if and to the extent that, and for as long as such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to:

1) avoid obstructing official or legally prescribed inquiries, investigations or procedures;

2) enable the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

3) protect public security;

4) protect national security and defence;

5) protect the rights and freedoms of others.

The law may prescribe that Para 3 of this Article shall apply, wholly or partially, to specific types of processing.

Right of access by the data subject

Article 26.

The data subject shall have the right to obtain from the controller information as to whether or not personal data concerning him or her are being processed, access to these personal data and the following information:

1) the purposes of the processing;

2) the categories of personal data processed;

3) the recipient or categories of recipients to whom the personal data have been or will be disclosed, and in particular recipients in third countries or international organisations;

4) the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

5) the existence of the right to request from the controller rectification or erasure of his or her personal data, or right to restriction of processing of personal data and right to object to such processing;

6) the right to lodge a complaint with the Commissioner;

7) available information about the source of personal data, if the personal data are not collected from the data subject;

8) the existence of automated decision-making procedure based on automated data processing, including profiling, referred to in Article 38 Paras 1 and 4 of this Law and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

If personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer pursuant to Article 65 of this Law.

The controller shall provide the data subject with a copy of the personal data undergoing processing. The controller may charge necessary fee based on administrative costs for any further copies requested by the data subject. If data subject makes the request for a copy by electronic means, the information shall be provided in a commonly used electronic form, unless otherwise requested by the data subject.

The rights and freedoms of others shall not be adversely affected by the right to obtain a copy referred to in Para 3 of this Article.

Provisions referred to in Paras 1 to 4 of this Article shall not apply to the processing of data by competent authorities for special purposes.

Right to access of the data subject whose data are processed by competent authorities for special purposes

Article 27.

Where personal data are processed by competent authorities for special purposes, the data subject shall have the right to obtain from the controller information as to whether or not personal data concerning him or her are being processed, and access to the personal data and the following information:

- 1) the purposes of and legal basis for the processing;
- 2) the categories of personal data processed;
- 3) the recipients or categories of recipients to whom the personal data have been disclosed, or will be disclosed, in particular recipients in third countries or international organisations;
- 4) the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- 5) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;
- 6) the right to lodge a complaint with the Commissioner and the contact details of the Commissioner;
- 7) communication of the personal data undergoing processing and of any available information as to their origin.

Limitations to the right of access

Article 28.

The right of access referred to in Article 27 of this Law may be restricted, wholly or partially, only in scope and duration, as long as such a partial or complete restriction

constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests, of the natural person concerned, in order to:

- 1) avoid obstructing official or legally prescribed inquiries, investigations or procedures;
- 2) enable the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- 3) protect public security;
- 4) protect national security and defence;
- 5) protect the rights and freedoms of others.

The law may prescribe that Para 1 of this Article shall apply, wholly or partially, to specific types of processing.

The controller shall inform the data subject in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction without undue delay and not later than within 15 days.

The controller shall not be obliged to act in line with Para 3 of this Article if that would undermine achieving a purpose for which the access was refused or restricted.

If Para 4 of this Article is applied on the decision on refusal of access, and if the procedure upon the applicant's request for access to data determines that information on the data subject is not processed, the controller shall, without undue delay and not later than within 15 days, inform the data subject that it is determined that there are no personal data in regards to which legally provided rights can be exercised and that he/she can lodge complaint with the Commissioner or the court if he/she deems that his or her rights have been breached.

The controller shall document the facts and the legal grounds for making the decision referred to in Para 1 of this Article, which shall be made available to the Commissioner at its request.

3. RIGHT TO RECTIFICATION, SUPPLEMENTATION, ERASURE, RESTRICTIONS AND PORTABILITY

Right to rectification and supplement

Article 29.

The data subject has the right to rectification of inaccurate personal data relating to him or her without delay. Taking into account the purposes of the processing, the data subject also has the right to have incomplete personal data relating to him or her completed, including by means of providing a supplementary statement.

Right to erasure of personal data

Article 30.

The data subject has the right to have the personal data concerning him or her erased by the controller.

The controller shall erase the data referred to in Para 1 of this Article without undue delay in the following cases:

- 1) personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- 2) the data subject has withdrawn the consent on which the processing is based according to Article 12 Para 1 Item 1) of this Law, or Article 17 Para 2 Item 1) of this Law and where there is no other legal ground for the processing;
- 3) the data subject objected to the processing pursuant to: a) Article 37 Para 1 of this Law, and there are no legitimate grounds for the processing overriding the interests, rights or freedoms of the data subject,
b) Article 37 Para 2 of this Law;
- 4) the personal data have been unlawfully processed;
- 5) the personal data have to be erased for compliance with a legal obligation of the controller prescribed by law;

6) the personal data have been collected in relation to the offer of information society services referred to in Article 16 Para 1 of this Law.

If the controller made personal data public, the controller's obligation to erase the personal data pursuant to Para 1 of this Article also involves undertaking all reasonable measures, taking account of the available technology and the ability to cover the cost of its implementation, to inform other controllers which are processing those personal data that the data subject submitted the request for erasure of all copies and references to or any electronic links to those personal data.

The data subject shall submit the request to exercise the right referred to in Para 1 of this Article to the controller.

Paras 1 to 3 of this Article shall not apply to the extent to which processing is necessary for:

- 1) exercising the right of freedom of expression and information;
- 2) compliance with a legal obligation of the controller prescribed by law, which require processing or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- 3) reasons of public interest in the area of public health in accordance with Article 17 Para 2 Items 8 and 9 of this Law;
- 4) archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 92 Para 1 of this Law, in so far as the exercise of the right referred to in Paras 1 and 2 of this Article is likely to render impossible or seriously impair the achievement of these objectives;
- 5) for the establishment, exercise or defence of legal claims.

Provisions referred to in Paras 1 to 5 of this Article shall not apply to the processing of data by competent authorities for special purposes.

Right to restriction of processing

Article 31.

The data subject shall have the right to restriction of processing of the data concerning him or her by the controller in the following cases:

1) data subject contested the accuracy of the personal data, for a period enabling the controller to verify the accuracy of the personal data;

2) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

3) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of a legal claim;

4) the data subject has objected to processing pursuant to Article 37 Para 1 of this Law, and the verification whether the legitimate grounds of the controller override the interests of the data subject is pending.

Where processing has been restricted under Para 1 of this Article, such personal data may further be processed, with the exception of storage, only with the data subject's consent, or for the purpose of the establishment, exercise or defence of legal claims, or for the protection of the rights of another natural, or legal person or for reasons of important public interest.

If data processing is restricted pursuant to Para 1 of this Article, the controller shall inform the data subject about the termination of restriction of processing, before the restriction of processing is lifted.

Provisions referred to in Paras 1 to 3 of this Article shall not apply to processing by competent authorities for special purposes.

Right to erasure and restriction of data processing by competent authorities for special purposes

Article 32.

Where personal data is processed by competent authorities for special purposes, the data subject has the right that personal data concerning him or her are erased by the controller, and the controller shall erase these data without undue delay, only in the case where the processing has breached the provisions of Articles 5, 13 and 18 of this Law, as well as when personal data must be erased in order to fulfil the legal obligation of the controller.

Instead of erasure, the controller shall restrict processing referred to in Para 1 of this Article in one of the following cases where:

- 1) the accuracy of the personal data is contested by the data subject, and their accuracy or inaccuracy cannot be ascertained;
- 2) the personal data must be collected and maintained for the purposes of evidence.

Where processing is restricted pursuant to Para 2 Item 1 of this Article, the controller shall inform the data subject of termination of restriction, prior to termination of the restriction.

Notification obligation regarding rectification, erasure or restriction of processing

Article 33.

The controller shall inform a recipient to whom the personal data have been disclosed of any rectification or erasure of personal data or restriction of their processing carried out in accordance with Article 29, Article 30 Para 1 and Article 31 of this Law, unless this proves impossible or involves disproportionate amount of time or resources.

The controller shall inform the data subject at his or her request, about the recipients referred to in Para 1 of this Article.

Provisions referred to in Paras 1 to 2 of this Article shall not apply to processing by competent authorities for special purposes.

Duty to inform about rectification, erasure and restriction of data processing by competent authorities for special purposes

Article 34.

Where personal data is processed by competent authorities for special purposes, the controller shall inform the data subject in writing about the decision on refusal to rectify, erase, or restrict the processing of data, as well as the reason for refusal.

The controller shall be wholly or partially released from the obligation to inform, referred to in Para 1 of this Article, to the extent to which that release of obligation constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to:

- 1) avoid obstructing official or legally prescribed inquiries, investigations or procedures;
- 2) enable the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- 3) protect public security;
- 4) protect national security and defence;
- 5) protect the rights and freedoms of others.

In the case referred to in Para 1 and 2 of this Article, the controller shall inform the data subject that he/she can address the Commissioner or the court.

The controller shall notify the competent authority from which this information was obtained of the rectification of incorrect data.

Where data was rectified, erased, or their processing was restricted pursuant to Article 29 and Article 32 Paras 1 and 2 of this law, the controller shall notify the data recipient of the rectification, erasure of these data, or the restriction of their processing.

The data recipient referred to in Para 5 of this Article shall rectify, erase the data, or restrict their processing.

Exercise of the rights of data subjects whose data is processed by competent authorities for special purposes and control of the Commissioner

Article 35.

In the cases referred to in Articles 25 Para 3, Article 28 Paras 3 and 4 and Article 34 Para 2 of this Law, the rights of the data subjects may be exercised through the Commissioner, and on the basis of its competencies prescribed by this Law.

The controller shall notify the data subject that in the cases referred to in Para 1 of this Article, he or she may exercise the rights through the Commissioner.

In the case referred to in Para 1 of this Article, the rights of data subjects are exercised through the Commissioner, the Commissioner shall notify the data subject at least as to the verification of the processing of data concerning him or her and control over data processing, as well as the right to address the court for the protection of his or her rights.

Right to data portability

Article 36.

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, if:

1) the processing is based on consent pursuant to Article 12 Para 1 Item 1 of this Law, or Article 17 Para 2 Item 1 of this Law, or based on a contract pursuant to Article 12 Para 1 Item 2; and if

2) the processing is carried out by automated means.

The right referred to in Para 1 of this Article, includes the right of the data subject that the personal data concerning him or her are transmitted directly from the controller to whom data was previously delivered to another controller, where technically feasible.

The exercise of the right referred to in Para 1 of this Article shall be without prejudice to the exercise of the right referred to in Article 30 of this Law. The right referred to in Para 1 of this Article shall not apply to processing necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.

The exercise of the right referred to in Para 1 of this Article shall not adversely affect the rights and freedoms of others.

Provisions referred to in Paras 1 to 4 of this Article shall not apply to processing by competent authorities for special purposes.

4. RIGHT TO OBJECT AND AUTOMATED INDIVIDUAL DECISION-MAKING

Right to object

Article 37.

The data subject shall have the right at any time to object, if he or she deems justified, on grounds relating to his or her particular situation, to processing of personal data concerning him or her, pursuant to Article 12 Para 1 Items 5 and 6 of this Law, including profiling based on those provisions. The controller shall cease the processing of personal data of the data subject who objected, unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Data subject shall have the right to object at any time to processing of personal data concerning him or her which are processed for direct marketing purposes, including profiling, to the extent that it is related to such direct marketing.

If the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

At the latest at the time of the first communication with the data subject, the controller shall explicitly bring to attention of the data subject the right referred to in Paras 1 and 2 of this Article and present it in an explicit and clear manner and separately from any other information provided.

In the context of the use of information society services, the data subject may exercise his or her right to object by automated means, using technical specifications for the use of services.

If personal data are processed for scientific or historical research purposes, or statistical purposes pursuant to Article 92 Para 1 of this Law, the data subject shall have the right to object to processing of these data, on the basis of his or her particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Automated individual decision-making and profiling

Article 38.

The data subject shall have the right that the decision made solely on the basis of automated processing, including profiling, is not applied to him or her, if such decision may produce legal effects concerning the data subject or significantly affect his or her legal position.

Para 1 of this Article shall not apply if the decision:

- 1) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
- 2) is based on law, if it lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests;
- 3) is based on the data subject's explicit consent.

In the cases referred to in Para 2 Items 1) and 3) of this Article, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller

in decision making process, or the right of the data subject, to express his or her point of view and to contest the decision before the authorized representative of the controller.

Decisions referred to in Para 2 of this Article shall not be based on special categories of personal data referred to in Article 17 Para 1, unless Article 17 Para 2 Items 1) and 5) of this Law applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Provisions referred to in Paras 1 to 4 of this Article shall not apply to processing by competent authorities for special purposes.

Automated individual decision-making and profiling in relation to data processing by
competent authorities for special purposes

Article 39.

It is forbidden to make the decision based solely on automated processing by competent authorities for special purposes, including profiling, if this decision may produce adverse legal effects concerning the data subject or significantly affect his or her position, unless if making this decision is based on law and if that law lays down suitable measures to safeguard the data subject's rights and freedoms, and at least the right to ensure the participation of a natural person in decision making.

The decision referred to in Para 1 of this Article shall not be based on special categories of personal data referred to in Article 18 Para 1 of this Law, unless appropriate measures are applied to safeguard the data subject's rights, freedoms and legitimate interests based on law.

Profiling which leads to discrimination of natural persons on the basis of special categories of personal data referred to in Article 18, Para 1 of this Law is prohibited.

5. RESTRICTIONS

Article 40.

The rights and obligations provided for in articles 21, 23, 24, 26, Articles 29 to 31, Article 33, Articles 36 to 39, Article 53, as well as Article 5 of this Law, if these provisions refer to the exercise of the rights and obligations provided for in Articles 21, 23, 24, 26, Articles 29 to 31, Article 33 and Articles 36 to 39 of this Law, may be restricted in so far as these restrictions respect the essence of the fundamental rights and freedoms and if it is a necessary and proportionate measure in a democratic society for:

- 1) the protection of national security;
- 2) defence;
- 3) the protection of public security;
- 4) the prevention and detection of criminal offences, and prosecution of criminal offenders or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
- 5) the protection of other important general public interests, and in particular important economic or financial interests of the Republic of Serbia, including monetary policy, budgetary and taxation matters, public health and social security systems;
- 6) judicial independence and judicial proceedings;
- 7) the prevention, investigation, detection and prosecution of breaches of professional ethics;
- 8) monitoring, inspection or regulatory function connected permanently or occasionally, to the exercise of official authority in the cases referred to in Items 1 to 5 and 7 of this Para;
- 9) the protection of the data subject or the rights and freedoms of others;
- 10) the enforcement of civil law claims.

When applying the restrictions of the rights and obligations referred to in Para 1 of this Article, it shall be taken into account, when relevant, at least:

- 1) the purposes of the processing and categories of processing;
- 2) the categories of personal data;
- 3) the scope of the restrictions;
- 4) the safeguards to prevent abuse, or unlawful access, or transfer of personal data;
- 5) the specification of the controller or categories of controllers;
- 6) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- 7) the risks to the rights and freedoms of data subjects;
- 8) the right of data subjects to be informed about the restriction, unless that may hinder the purpose of the restriction.

Provisions referred to in Paras 1 and 2 of this Article shall also apply to processing by competent authorities which is not performed for special purposes.

IV. CONTROLLER AND PROCESSOR

1. GENERAL OBLIGATIONS

Responsibility of the controller

Article. 41.

The controller shall implement appropriate technical, staffing and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Law, taking into account the nature, scope, context and purposes of processing, as

well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

The measures referred to in Para 1 shall be reviewed and updated where necessary.

If it is proportional in respect of data processing, measures referred to in Para 1 of this Article include the application of appropriate internal rules of the controller on protection of personal data.

The controller may demonstrate compliance with the obligations referred to in Para 1 of this Article and on the basis of adherence to approved codes of conduct as referred to in Article 59 of this Law, or issued certificate as referred to in Article 61 of this Law.

Provisions referred to in Para 4 of this Article shall not apply to processing by competent authorities for special purposes.

Protection measures

Article 42.

Taking into consideration available technology and costs of its implementation, the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself:

1) implement in an effective manner appropriate technical, organisational and staffing measures, such as pseudonymisation, for ensuring implementation of the principles of personal data processing;

2) ensure implementation of the necessary safeguards in the course of processing, in order to meet the requirements for data processing prescribed by this Law and protection of the rights and freedoms of the data subject.

The controller shall, by constantly implementing appropriate technical, organisational and staffing measures ensure that, by default, only personal data which are necessary for achieving each single purpose of the processing are processed. That obligation applies in

relation to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Measures referred to in Para 2 of this Article shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

The controller may demonstrate compliance with the requirements set out in Paras 1 to 3 of this Article on the basis of the issued certificate pursuant to Article 61 of this Law.

Provision referred to in Para 4 of this Article shall not apply to processing by competent authorities for special purposes.

Joint controllers

Article 43.

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

Joint controllers referred to in Para 1 of this Article shall, in a transparent manner, determine their respective responsibilities for compliance with the provisions prescribed by this Law, and in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information to data subject referred to in Articles 23 to 25 of this Law.

Responsibility referred to in Para 2 of this Article shall be determined by an arrangement between joint controllers, unless this responsibility is determined by law to which the controllers are subject to.

The arrangement referred to in Para 3 of this Article must designate a contact point for data subjects and regulate the relationships of each of the joint controllers vis-à-vis the data subjects.

The essence of the provisions of the arrangement referred to in Para 3 of this Article must be available to the data subject.

The provisions referred to in Paras 4 and 5 of this Article shall not apply to the processing by competent authorities for special purposes.

Irrespective of the terms of the arrangement referred to in Para 3 of this Article, the data subject may exercise his or her rights under this Law, in respect of and against each of the controllers individually.

Representatives of controllers or processors not established in the Republic of Serbia

Article 44.

In cases referred to in Article 3 Para 4 of this Law, the controller or the processor, shall designate in writing its representative in the Republic of Serbia, unless if:

1) processing is occasional and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing, and it does not include, on a large scale, processing of special categories of data as referred to in Article 17 Para 1 of this Law, or processing of personal data relating to criminal convictions and offences referred to in Article 19 of this Law;

2) the controller or the processor is a public authority body.

The controller or the processor shall mandate the representative referred to in Para 1 of this Article as the person the data subject, the Commissioner, or other person may address, in addition to or instead of the controller or the processor, on all issues related to processing, for the purposes of ensuring compliance with the provisions of this Law.

Complaint, lawsuit or other legal actions referred to in this Law, could be lodged against the controller or the processor without prejudice to the designation of their representative referred to in Para 1 of this Article.

Processor

Article 45.

Where data processing is performed on behalf of the controller, the controller may designate as the processor only the person who fully guarantees implementation of appropriate technical, staffing and organisational measures, in a manner that ensures processing is performed in line with the provisions of this Law and the protection of the rights of the data subject.

The processor referred to in Para 1 of this Article may engage another processor only on the basis of prior specific or general written authorisation of the controller. In the case of processing based on general written authorisation, the processor shall inform the controller of any intended selection of another processor, or replace another processor, giving the controller the opportunity to object to such changes.

Processing by a processor shall be governed by a contract or other legally binding act, concluded or adopted in a written form, including in electronic form, which, pursuant to the law, governs the relationship between the controller and the processor, and sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

The contract or other legally binding act referred to in Para 3 of this Article shall stipulate that the processor:

- 1) processes the personal data only on the basis of documented instructions from the controller, including and with regard to transfers of personal data to third countries or an international organisation, unless if the processor is obliged by law to process the data. In such a case, the processor shall inform the controller of that legal requirement prior to initiation of processing, unless if law prohibits delivery of such information on important grounds of public interest;

- 2) ensures that persons authorised to process the personal data have committed themselves to confidentiality, or are under an appropriate statutory obligation of confidentiality;

- 3) takes all measures required, pursuant to Article 50 of this Law;

4) respects the conditions for engaging another processor referred to in Paras 2 and 7 of this Article;

5) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of this Law;

6) assists the controller in ensuring compliance with the obligations pursuant to Article 50 and Articles 52 to 55 of this Law, taking into account the nature of processing and the information available to the processor;

7) after the end of the contracted processing actions, and on the basis of the decision of the controller, deletes or returns all the personal data to the controller, and deletes existing copies of data, unless the law requires storage of the personal data;

8) makes available to the controller all information necessary to demonstrate compliance with the obligations of the processor laid down in this Article, as well as information which allows for and contributes to audits, conducted by the controller or another auditor mandated by the controller.

In the case referred to in Para 4 Item 8 of this Article, the processor shall inform the controller, without undue delay, if it deems that the written instruction received from the controller is not in line with this Law or other law governing personal data protection.

In case of processing by competent authorities for special purposes, the contract or other legally binding act referred to in Para 3 of this Article shall prescribe that the processor is obliged to:

1) process the personal data only on basis of the instructions from the controller;

2) ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3) assist in an appropriate manner the controller in fulfilling its obligation of compliance with the provisions on the rights of data subjects referred to in Chapter III of this Law;

4) after the end of the contracted processing actions, and on the basis of the decision of the controller, delete or return all the personal data to the controller, and delete existing copies of data, unless the law requires storage of the personal data;

5) make available to the controller all information necessary to demonstrate compliance with the obligations of the processor laid down in this Article;

6) ensure fulfilment of the conditions laid down in Paras 2, 3 and 6 of this Article also in the case it designates data processing to another processor.

Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same obligations of personal data protection prescribed by the contract or other legally binding act concluded between the controller and the processor referred to in Paras 3 and 4 of this Article, impose obligations to another processor based on the contract or other legally binding act, concluded or adopted in a written form, including electronic form, in the relationship between the controller and the processor, which prescribes sufficient safeguards for implementation of appropriate technical, staffing and organisational measures that ensure data processing is performed in line with this Law. If another processor fails to meet its obligations in relation to personal data processing, the processor shall remain fully liable for the performance of these obligations of another processor.

Where the processor breaches the provisions of this Law by determining the purpose and means of processing, the processor shall be considered to be a controller in respect of that processing.

Fulfilment of responsibilities of provision of safeguards referred to in Paras 1 and 7 of this Article may also be demonstrated on the basis of adherence of a processor to an approved code of conduct, as referred to in Article 59 of this Law, or an issued certificate, referred to in Article 61 of this Law.

The legal relationship between the controller and the processor, prescribed in line with Paras 3 and 7 of this Article may be based, in whole or in part, on standard contractual clauses referred to in Para 11 of this Article, including those related to the certificate granted to the controller or processor pursuant to Articles 61 and 62 of this Law.

The Commissioner may lay down standard contractual clauses for the matters referring to responsibilities laid down in Paras 3 and 7 of this Article, in particular taking into account the european practice in developing standard contractual clauses.

The provisions referred to in Paras 4, 5, 7 and Paras 9 to 11 of this Article shall not apply to the processing by competent authorities for special purposes.

Processing under the authority or instructions

Article 46.

The processor, or any person acting under the authority of the controller or of the processor to access personal data, may process those data only on the basis of instructions from the controller, or if it is obliged by law.

Records of processing activities

Article 47.

Each controller and the controller's representative shall maintain a record of processing activities under its responsibility, containing all of the following information on:

- 1) the controller and, where applicable, the joint controller, the or the joint controllers, the controller's representative and the data protection officer, their title or the name and contact details;
- 2) the purposes of the processing;
- 3) the categories of data subjects and the categories of personal data;
- 4) the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations;
- 5) where applicable, transfers of personal data to third countries or an international organisation, including the identification of that third country or international organisation, and, in the case of transfers referred to in Article 69 Para 2 of this Law, the documentation of suitable safeguards;

6) where possible, the envisaged time limits for erasure of the different categories of personal data;

7) where possible, a general description of security measures referred to in Article 50 Para 1 of this Law.

Provisions of Para 1 of this Article shall not apply to data processing by competent authorities for special purposes.

In case of data processing by competent authorities for special purposes, the controller shall maintain a record of processing activities under its responsibility, containing all of the following information on:

1) the controller and, where applicable, the joint controllers, and the data protection officer, their title or the name and contact details;

2) the purposes of the processing;

3) the categories of data subjects and the categories of personal data;

4) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

5) where applicable, the use of profiling;

6) where applicable, types of transfers of personal data to third countries or international organisations;

7) the legal grounds for the processing of personal data, including their transfer;

8) where possible, the envisaged time limits for erasure of the different categories of personal data;

9) where possible, a general description of the security measures referred to in Article 50 Para 1 of this Law.

Each processor, and where applicable, its representative, shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing data on:

1) the processor, or processors and of each controller on behalf of which the processing is carried out, and, where applicable, of the controller's or the processor's representative, and the data protection officer: their title, the name and contact details;

2) the categories of processing carried out on behalf of each controller;

3) where applicable, transfers of personal data to third countries or international organisations, including the identification of that third country or international organisation,

and, in the case of transfers referred to in Article 69 Para 2 of this Law, the documentation of suitable safeguards;

4) where possible, a general description of the security measures referred to in Article 50 Para 1 of this Law.

Provisions of Para 4 of this Article shall not apply to data processing by competent authorities for special purposes.

Where processing is carried out by competent authorities for special purposes, each processor shall maintain a record of all categories of data processing activities carried out on behalf of a controller, containing data on:

1) each processor, and each controllers on behalf of which the processing is carried out, and of the data protection officer: their title, the name and contact details;

2) the categories of processing carried out on behalf of each controller;

3) where applicable, transfers of personal data to third countries or international organisations where explicitly instructed to do so by the controller, including identification of that third country or international organisation;

4) where possible, a general description of security measures referred to in Article 50 Para 1 of this Law.

The records referred to in Paras 1, 3, 4 and 6 of this Article shall be in writing, including in electronic form and shall be kept permanently.

The controller and, where applicable, the processor, or their representatives, shall make the record referred to in Paras 1, 3, 4 and 6 of this Article available to the Commissioner on its request.

The provisions referred to in Paras 1 and 4 of this Article shall not apply to business entity and organisations employing fewer than 250 persons unless:

1) the processing they carry out is likely to result in a risk to the rights and freedoms of data subjects; or

2) the processing is not occasional; or,

3) the processing includes special categories of data as referred to in Article 17 Para 1 of this Law, or personal data relating to criminal convictions, offences and security measures, referred to in Article 19 of this Law.

Logging of processing operations by competent authorities for special purposes

Article 48.

The competent authority processing data for special purposes shall ensure that logs are kept for at least the following processing operations in automated processing systems: collection, alteration, consultation, disclosure including transfers, combination and erasure.

The logs of consultation and disclosure shall enable the determination of the justification for processing, establishment of date and time of such operations, and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data.

The logging referred to in Para 1 of this Article shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for the initiation and conduct of the criminal proceedings.

The record created by logging referred to in Para 1 of this Article shall be made available to the Commissioner on request, pursuant to law.

Cooperation with the Commissioner

Article 49.

The controller and the processor and where applicable, their representatives, shall cooperate with the Commissioner in the performance of its tasks.

2. Security of personal data

Security of processing

Article 50.

Taking into consideration available technology and costs of its implementation, the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical, staffing and organisational measures to ensure a level of security appropriate to the risk.

Where it is necessary, the measures referred to in Para 1 of this Article shall in particular include:

- 1) the pseudonymisation and encryption of personal data;
- 2) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of personal data processing systems and services;
- 3); the ability to restore the availability and access to personal data in a timely manner, in the event of a physical or technical incident;
- 4) a process for regularly testing, assessing and evaluating the effectiveness of technical, staffing and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security referred to in Para 1 of this Article, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Adherence to an approved code of conduct as referred to in Article 59 of this Law or an issued certificate, as referred to in Article 61 of this Law, may be used to demonstrate compliance with the requirements set out in Para 1 of this Article.

The controller and processor shall take steps to ensure that natural person acting under the authority of the controller or the processor who has access to personal data, processes these data only on the basis of instructions from the controller or when it is obliged by law.

Provisions of Paras 1 to 5 of this Article shall not apply to data processing by competent authorities for special purposes.

Security of data processing by competent authorities for special purposes

Article 51.

Where data processing is carried out by competent authorities for special purposes, and in line with available technology and the costs of its implementation, the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical, staffing and organisational measures to ensure a level of security appropriate to the risk, and in particular as regards the processing of special categories of personal data referred to in Article 18 of this Law.

Based on the risk assessment, the controller or processor shall implement, in respect of automated processing, appropriate measures referred to in Para 1 of this Article designed to:

- 1) deny unauthorised persons access to processing equipment used for processing ('equipment access control');
- 2) prevent the unauthorised reading, copying, modification or removal of data media ('data media control');
- 3) prevent the unauthorised input of personal data and the unauthorised modification, deletion or inspection of stored personal data ('storage control');
- 4) prevent the use of automated processing systems by unauthorised persons using data communication equipment ('user control');
- 5) ensure that persons authorised to use an automated processing system have access only to the personal data covered by their access authorisation ('data access control');

6) ensure that it is possible to verify and establish to whom the personal data have been or may be transmitted or made available using data communication equipment ('communication control');

7) ensure that it is subsequently possible to verify and establish which personal data have been input into automated processing systems and when and by whom the personal data were input ('input control');

8) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media ('transport control');

9) restore installed systems in the case of interruption of their work ('recovery');

10) ensure that the functions of the system perform, that the appearance of faults in the functions is reported ('reliability') and that stored personal data cannot be corrupted by means of a malfunctioning of the system ('integrity').

Notification of the Commissioner about personal data breach

Article 52.

In the case of a personal data breach, which may result in a risk to the rights and freedoms of natural persons, the controller shall notify the Commissioner without undue delay and, where feasible, not later than 72 hours after having become aware of it.

If the controller does not act within 72 hours after having become aware of the personal data breach, reasons for the delay must be stated.

The processor shall notify the controller, without undue delay, after becoming aware of a personal data breach.

The notification referred to in Para 1 of this Article shall contain at least the following information:

1) description of nature of the personal data breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

2) the name and contact details of the data protection officer, or other contact point, where more information can be obtained;

3) description of the likely consequences of the personal data breach;

4) description of the measures taken, or proposed to be taken by the controller to address the personal data breach, including measures to mitigate its possible adverse effects.

If it is not possible to provide information referred to in Para 4 of this Article at the same time, the controller shall provide the information without undue further delay and in phases.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

Documentation referred to in Para 6 of this Article shall represent the grounds enabling the Commissioner to verify whether the controller has complied with the provisions of this Article.

Where the breach of personal data processed by competent authorities for special purposes involves personal data that have been transmitted to the controller of another state or international organization, the controller shall communicate, without undue delay, the information referred to in Para 4 of this Article to the controller of another state or international organization, pursuant to international agreement.

The Commissioner shall prescribe the form for the notification referred to in Para 1 of this Article and specify the methods of notification.

Communication of a personal data breach to the data subject

Article 53.

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

In the communication to the data subject referred to in Para 1 of this Article, the controller shall describe in clear and plain language the nature of the personal data breach and provide at least the information referred to in Article 52 Para 4 Items 2 to 4 of this Law.

The controller shall not be required to communicate to the data subject referred to in Para 1 of this Article if:

1) the controller has implemented appropriate technical, organisational and staffing protection measures, in relation to the personal data affected by the personal data breach, and in particular if encryption or other measures prevented readability of the personal data to any unauthorized persons for access to this data;

2) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

3) if communicating the personal data breach to the data subject would involve disproportionate amount of time and resources, in which case the controller shall utilise a public communication through the media or similar equally effective method to ensure the data subjects are informed.

Having considered the likelihood of the personal data breach resulting in a high risk to the rights and freedoms of data subjects, the Commissioner may require the controller who has not already communicated the personal data breach to the data subject to do so, or may determine that any of the conditions referred to in Para 3 of this Article are met.

In the case of breach of personal data processed by competent authorities for special purposes, the controller may delay, or restrict communication to the data subject, on the grounds and under the conditions referred to in Article 25 Para 3 of this Law.

3. Impact assessment of processing to data protection and prior opinion of the Commissioner

Data protection impact assessment

Article 54.

Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an impact assessment of the envisaged processing operations on the protection of personal data.

Impact of a set of similar processing operations that present similar high risks for data protection may be addressed by a single assessment.

When carrying out impact assessment, the controller shall seek the advice of the data protection officer, where designated.

Impact assessment referred to in Para 1 of this Article shall in particular be required in the case of:

- 1) a systematic and extensive evaluation of personal aspects relating to natural persons based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

- 2) processing on a large scale of special categories of personal data referred to in Article 17 Para 1, Article 18 Para 1, and Article 19 of this Law;

- 3) a systematic monitoring of a publicly accessible area on a large scale.

The Commissioner shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to Para 1 of this Article and may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required.

The impact assessment shall contain at least:

- 1) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest of the controller to process the data;

- 2) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

3) an assessment of the risks to the rights and freedoms of data subjects referred to in Para 1 of this Article;

4) a description of the measures envisaged to address the risks referred to in Para 1 of this Article, including legal safeguards, security measures and technical, organizational and staffing measures aimed to ensure the protection of personal data and to demonstrate compliance with this Law, in particular taking into account the rights and legitimate interests of data subjects and other persons concerned.

The provisions of Para 6 of this Article shall not apply to impact assessment of personal data processed by competent authorities for special purposes.

The impact assessment of personal data processed by competent authorities for special purposes shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects referred to in Para 1 of this Article, as well as the measures envisaged to address the risks referred to in Para 1 of this Article, including legal safeguards, security measures and technical, organizational and staffing measures, aimed to ensure the protection of personal data and to demonstrate compliance with this Law, in particular taking into account the rights and legitimate interests of the data subjects and other persons concerned.

Compliance with approved codes of conduct referred to in Article 59 of this Law by the controller or processor shall be taken into due account in assessing the impact of the processing operations.

Provisions of Para 9 of this Article shall not apply to data processing by competent authorities for special purposes.

Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing operations, without prejudice to the protection of commercial or public interests or the security of processing operations.

If a special law regulates the specific processing operation or set of processing operations, data protection impact assessment shall be previously carried out as part of a general impact assessment prescribed. In such a case, Paras 1 to 9 of this Article shall not

apply, where processing is performed pursuant to Article 12 Para 1 Items 3 or 5 of this Law, unless the controller deems necessary to carry out new assessment.

Where necessary, and at least when there is change of the level of risk related to processing operations, the controller shall carry out a review to assess if processing is performed in accordance with the performed data protection impact assessment.

Prior consultation and attaining opinion from the Commissioner

Article 55.

Where a data protection impact assessment, performed under Article 54 of this Law, indicates that the envisaged processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, the controller shall consult the Commissioner prior to processing.

The provision of Para 1 of this Article shall not apply in case of processing personal data by competent authorities for special purposes.

In case of processing personal data by competent authorities for special purposes, the controller or processor shall consult the Commissioner prior to processing actions which will form part of a new filing system to be created, where:

- 1) a data protection impact assessment carried out pursuant to Article 54 of this Law indicates that the envisaged processing operations would result in a high risk in the absence of measures taken by the controller to mitigate the risk; or
- 2) the type of processing, in particular, where using new technologies, mechanisms or procedures, involves a high risk to the rights and freedoms of data subjects.

If the Commissioner is of the opinion that the intended processing operations referred to in Para 1 and 3 of this Article would infringe this Law, in particular where the controller has insufficiently identified or mitigated the risk, the Commissioner shall, within period of up to 60 days of receipt of the request for prior consultation, provide written advice to the controller and, where applicable, to the processor, on personal data processing and may use any of its powers referred to in Article 79 of this Law.

That period referred to in Para 4 of this Article may be extended by 45 days, taking into account the complexity of the intended processing operations and the Commissioner shall inform the controller and the processor, of any such extension and the reasons for the delay within 30 days of receipt of the request for consultation.

The periods referred to in Paras 4 and 5 of this Article shall be suspended in the period in which the Commissioner is waiting for the controller and the processor to deliver the information requested which is necessary for the purposes of the provision of the consultation.

Along with the consultation, the controller shall provide the Commissioner information on:

- 1) the respective responsibilities of the controller, and where applicable, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
- 2) the purposes and means of the intended processing;
- 3) the technical, organizational and staffing measures and legal safeguard mechanisms provided to protect the rights and freedoms of data subjects, which are implemented pursuant to this Law;
- 4) where applicable, the contact details of the data protection officer;
- 5) the data protection impact assessment provided for in Article 54 of this Law;
- 6) any other information requested by the Commissioner.

The provisions of Para 7 of this Article shall not apply to processing personal data by competent authorities for special purposes.

In case of processing personal data by competent authorities for special purposes, the controller referred to in Para 3 of this Article shall provide the Commissioner with information on personal data impact assessment referred to in Article 54 of this Law, and other information relevant for the consultation by the Commissioner, at its request on

processing operations, and in particular the risks to for the personal data of data subjects and mechanisms of protection of their rights.

The Commissioner may develop and make publicly available the list of processing operations that require its opinion.

Public authority bodies proposing the adoption of legislative or other acts based on laws that contain provisions on personal data processing shall request opinion of the Commissioner during the drafting process.

4. DATA PROTECTION OFFICER

Designation of the data protection officer

Article 56.

4. DATA PROTECTION OFFICER

Designation of the data protection officer

Article 56.

The controller and the processor may designate a data protection officer.

The controller and the processor shall designate a data protection officer in any case where:

1) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

2) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;

3) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 17 Para 1 and personal data referred to in Article 19 of this Law.

The provisions of Paras 1 and 2 of this Article shall not apply in case of processing personal data by competent authorities for special purposes.

Where processing personal data is carried out by competent authorities for special purposes, the controller shall designate a data protection officer, except if processing is carried out by courts when acting in their judicial capacity.

A group of undertakings may appoint a single data protection officer, provided that a data protection officer is easily accessible to each member of the group.

Where the controller or the processor is public authority body, but not competent authorities, a single data protection officer may be designated taking account of their size and organisational structure.

Competent authorities may designate a single data protection officer, taking into account their size and organisational structure.

Special law may prescribe that the controllers or the processors, or associations representing them, are required to designate a data protection officer.

The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge in the field of data protection and the ability to fulfil the tasks referred to in Article 58 of this Law.

The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

The controller or the processor shall publish the contact details of the data protection officer and communicate them to the Commissioner.

The Commissioner shall keep the record of data protection officers, which shall include: first and last names of data protection officers, their contact details, and names and contact details of the controller or processor.

The Commissioner shall prescribe the form of the record referred to in Para 11 of this Article and shall regulate the manner of its keeping.

Position of the data protection officer

Article 57.

The controller and the processor shall involve the data protection officer, properly and in a timely manner, in all issues which relate to the protection of personal data.

The controller and the processor shall enable the data protection officer to perform the tasks referred to in Article 58 of this Law, by providing resources necessary to carry out those tasks, access to personal data and processing operations, as well as to maintain his or her expert knowledge.

The controller and processor shall ensure the independence of the data protection officer.

The controller and processor shall not penalise or dismiss the data protection officer for performing its tasks referred to in Article 58 of this Law.

The data protection officer shall directly report for performing his tasks referred to in Article 58 of this Law to the highest management level of the controller or the processor.

Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Law.

The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, referred to in Article 58 of this Law, pursuant to law.

The data protection officer may fulfil other tasks and duties, and the controller or the processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Where controllers are competent authorities processing data for special purposes, the provisions of Paras 1 to 5 and 8 of this Article shall not apply to the processor.

Tasks of the data protection officer

Article 58.

The data protection officer shall at least have the following tasks:

1) to inform and advise the controller or the processor and the employees who carry out processing of their legal obligations concerning personal data protection;

2) to monitor compliance with this Law, other laws and with the internal policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

3) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 54 of this Law;

4) to cooperate with the Commissioner, represent the contact point for cooperation with the Commissioner, and to consult with the Commissioner, on issues relating to processing, including the prior consultation and attaining opinion referred to in Article 55, of this Law;

The data protection officer shall, in the performance of its tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Where controllers are competent authorities processing data for special purposes, the provisions of Para 1 Items 1 and 2 of this Article shall not apply to the processor.

5. CODES OF CONDUCT AND CERTIFICATION

Codes of conduct

Article 59.

Associations and other bodies representing categories of controllers or processors may adopt codes of conduct, for the purpose of effective implementation of this Law, in particular with regard to:

1) fair and transparent processing;

2) the legitimate interests pursued by controllers, taking into account the specific contexts;

3) the collection of personal data;

4) the pseudonymisation of personal data;

5) the information provided to the public and to data subjects;

6) the exercise of the rights of data subjects;

7) the information provided to children, their protection, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;

8) the measures and procedures referred to in Articles 41 and 42 of this Law and the measures to ensure security of processing referred to in Article 50 of this Law;

9) the notification of personal data breaches to the Commissioner and the communication of such personal data breaches to data subjects;

10) the transfer of personal data to third countries or international organisations;

11) methods of peaceful dispute resolution for resolving disputes between controllers and data subjects, without prejudice to the rights of data subjects pursuant to Articles 82 and 84 of this Law.

In order to provide appropriate safeguards to data subjects concerning their personal data transfers to third countries or international organisations under the terms referred to in Article 65 Para 2 Item 3) of this Law, the controllers or processors that are not subject to this Law may also commit or adhere to the implementation of the code of conduct approved pursuant to Para 5 of this Article, via contractual or other legally binding instruments, to guarantee implementation of all appropriate safeguards, and in particular in relation to data subjects.

A code of conduct referred to in Para 1 of this Article shall contain provisions which enable the person referred to in Article 60 Para 1 of this Law to carry out the monitoring of compliance with its provisions by the controllers or processors, who adhered to the

implementation of the code of conduct, without prejudice to the control powers and other powers of the Commissioner pursuant to Articles 77 to 79 of this Law.

Associations and other bodies referred to in Para 1 of this Article which intend to develop codes of conduct or amend the existing ones, shall submit the draft code of conduct or its amendments for the opinion of the Commissioner.

The Commissioner shall provide an opinion on compliance of the proposal of the code or its amendments with the provisions of this Law, and if it determines that the draft code contains sufficient personal data protection safeguards, register and publish the Code of conduct or its amendments on its website.

Provisions of Paras 1 to 5 of this Article shall not apply to processing performed by competent authorities for special purposes.

Monitoring of the implementation of codes of conduct

Article 60.

Monitoring of the implementation of codes of conduct, pursuant to Article 59 Para 3 of this Law, may be carried out by an entrepreneur or a legal person who is accredited for monitoring pursuant to the law governing accreditation.

Monitoring of compliance referred to in Para 1 of this Article does not affect the general authority, tasks, monitoring and other powers of the Commissioner under Articles 77 to 79 of this Law.

The entrepreneur or a legal person referred to in Para 1 of this Article may be accredited only if it has:

1) demonstrated its independence and expertise in relation to the subject-matter of the code, pursuant to the opinion of the Commissioner;

2) established procedures which allow it to assess the eligibility of controllers and processors for implementation of the code, to monitor their compliance with its provisions and to periodically review its effectiveness;

3) established procedures and structures to decide upon complaints about infringements of the code or the manner in which the code is being implemented by a

controller or processor, and to make those procedures and structures transparent to data subjects and the public;

4) demonstrated that its tasks and duties do not result in a conflict of interests, pursuant to the opinion of the Commissioner.

An entrepreneur, or a legal person referred to in Para 1 of this Article, shall take appropriate action in prescribed proceedings in cases of infringement of the code by a controller or processor, including temporary suspension or exclusion of the controller or processor concerned from the implementation of the code.

An entrepreneur, or a legal person referred to in Para 1 of this Article, shall inform the Commissioner of undertaken measures referred to in Para 4 of this Article and the reasons for undertaking them.

Undertaking measures referred to in Para 4 of this Article shall be without prejudice to the tasks and powers of the Commissioner and the provisions of Chapter VII of this Law.

The accreditation of an entrepreneur, or a legal person referred to in Para 1 of this Article shall be revoked if it is determined that the conditions for accreditation are no longer met or where actions it takes infringe this Law.

Provisions of Paras 1 to 7 of this Article shall not apply to processing carried out by public authority bodies or competent authorities processing data for special purposes.

Certification

Article 61.

Taking into account the specific needs of small and medium-sized enterprises, the data protection certification mechanisms and data protection seals and marks may be established, for the purpose of demonstrating compliance with this Law by controllers and processors.

Within the framework of personal data transfers to third countries or international organisations, under the terms referred to in Article 65 Para 2 Item 4 of this Law, a certificate may be issued with appropriate seals and marks, pursuant to Para 5 of this Article, to controllers or processors that are not subject to this Law, for the purpose of demonstrating the existence of appropriate safeguards, if they make binding and enforceable commitments,

via contractual or other legally binding acts, to apply these appropriate safeguards, including with regard to the rights of data subjects.

The certification procedure shall be voluntary and transparent.

Possession of an issued certificate pursuant to Para 1 of this Article does not reduce the responsibility of the controller and the processor for compliance with this Law and is without prejudice to the general authority, tasks, monitoring and other powers of the Commissioner pursuant to Articles 77 to 79 of this Law.

Certification shall be issued by certification body referred to in Article 62 of this Law or the Commissioner, on the basis of criteria approved by the Commissioner, pursuant to powers prescribed in Article 79 Para 3 of this Law.

The controller and the processor, requesting issuance of the certificate, shall provide the certification body referred to in Article 62 of this Law, or the Commissioner, if the request is addressed at the Commissioner, with all information and access to its processing activities which are necessary to conduct the certification procedure.

Certification shall be issued to a controller or processor for a maximum period of three years and may be renewed, under the prescribed conditions.

Certification referred to in Para 7 of this Article shall be annulled, if the certification body or the Commissioner, if the request is addressed at the Commissioner, determine that the controller or the processor do no longer meet the requirements for the certification.

The Commissioner shall maintain and publish on the website a public register of all certification bodies and mechanisms, with appropriate seals and marks.

Provisions of Paras 1 to 9 of this Article shall not apply to processing carried out by competent authorities for special purposes.

Certification bodies

Article 62.

The certification body, which has an appropriate level of expertise in relation to data protection and is accredited pursuant to law governing accreditation, shall issue, renew and

withdraw the certificate, along with the seals and marks, after informing the Commissioner of the decision it plans to make, without prejudice to general authority, tasks, monitoring and other powers of the Commissioner pursuant to Articles 77 to 79 of this Law.

Certification bodies referred to in Para 1 of this Article shall be accredited only if they have:

1) demonstrated their independence and expertise in relation to the subject-matter of the certification pursuant to the opinion of the Commissioner;

2) undertaken to respect the criteria referred to in Article 61 Para 5 of this Law;

3) established procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;

4) established procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public;

5) demonstrated that their tasks and duties do not result in a conflict of interests pursuant to the opinion of the Commissioner.

The Commissioner shall determine the criteria for accreditation of certification bodies pursuant to conditions referred to in Para 2 of this Article.

The accreditation of certification bodies shall be issued to a maximum period of five years and may be renewed, if the certification body continues to meet the prescribed conditions.

The accreditation of the certification body shall be withdrawn if it is determined that it no longer meets the requirements or the accreditation criteria or if it is determined that the certification body violated the provisions of this Law.

The certification bodies shall be responsible for appropriate assessment of the fulfilment of criteria for issuing, renewing and withdrawing the certificate and shall provide the Commissioner with the reasons for issuing, granting or withdrawing the requested certification.

The Commissioner shall publish the criteria for accreditation referred to in paragraph 3 of this Article.

Certificates issued by certification bodies of other countries or international organisations shall be recognized provided it was issued in accordance with the ratified international agreements signed by the Republic of Serbia.

If the certification body which conducted certification was accredited by a national body of another country, which signed an agreement with the Accreditation Body of Serbia, mutually recognizing the equivalence of the accreditation systems to the extent determined by the signed agreement, certificates of that certification body may be accepted in the Republic of Serbia, without conducting a new certification process.

Provisions of Paras 1 to 8 of this Article shall not apply to processing carried out by competent authorities for special purposes.

V. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

General principles

Article 63.

Any transfer of personal data which are undergoing processing, or personal data that are intended for processing after transfer to a third country or to an international organisation, shall take place only if, subject to the other provisions of this Law, the controller and processor act in line with the conditions laid down in this Chapter, including the case of onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation, in order to ensure that the level of protection of natural persons is equal to the one guaranteed by this Law.

Where processing is carried out by competent authorities for special purposes, the transfer of personal data, which are currently processed or which are intended for further processing following transfer to a third country or an international organisation, can be performed only where the following conditions are jointly met:

1) the transfer is necessary for special purposes;

2) the personal data are transferred to a controller in a third country or international organisation that is an authority competent for performing functions for special purposes;

3) the government has adopted a list of countries or parts of their territories, fields of actions, or legal regulation and international organisations that ensure appropriate level of personal data protection in line with Article 64 of this Law, and transfer of personal data is performed in one of these countries, or parts of their territories, fields of actions or legal regulation and an international organisation, or where that is not the case, implementation of appropriate safeguards is ensured pursuant to Article 66 of this Law, or where their implementation is not ensured, provisions of Article 70 of this Law on transfers of personal data in specific situations shall apply;

4) in the case of an onward transfer from a third country or international organization to another third country or international organisation, the competent authority that carried out the original transfer, or another competent authority of the Republic of Serbia, authorises the onward transfer, after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose of the first transfer of the personal data and the level of personal data protection in the third country or an international organisation to which personal data is further transferred.

Transfer on the basis of appropriate level of safeguards

Article 64.

A transfer of personal data to a third country, parts of its territory, areas of activity or legal regulation or an international organisation, without prior approval, may take place if it is determined that the third country, parts of their territory or areas of activity or legal regulation within that third country, or the international organisation in question, ensure an adequate level of protection of personal data.

It is considered that the appropriate level of protection referred to in Para 1 of this Article is ensured in the countries and international organizations which are members of the Council of Europe Convention on the Protection of Individuals with regard to Automatic Personal Data Processing, or in the countries, parts of their territories, areas of activity or

legal regulation, or international organizations for which the European Union has determined that they provide an adequate level of protection.

The Government may determine that the State, part of its territory, area of activity or legal regulation or an international organization does not provide the appropriate level of protection referred to in Para 1 of this Article, except for the members of the Council of Europe Convention on the Protection of Individuals with regard to Automatic Personal Data Processing, taking into account:

1) the principle of the rule of law and respect for human rights and fundamental freedoms, relevant legislation, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules and professional rules in this field, security measures, including rules for the onward transfer of personal data to third countries or international organisations which are implemented in the practice of courts and other public authority bodies within that third country, or the international organisation, as well as the effectiveness of the exercise of rights of data subjects and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

2) the existence and effective functioning of supervisory authority for personal data protection in the third country or supervisory authority competent for supervision over international organizations in this field, authorized to ensure and enforce compliance with the data protection rules and initiate mechanisms of data protection in case of their breaches, to assist and advise the data subjects to exercise their rights and to cooperate with the Commissioner;

3) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding international conventions or instruments, as well as from its participation in multilateral or regional organizations, in particular in relation to the protection of personal data.

It is considered that an adequate level of protection of personal data ALSO exists if an international agreement with the third country, or an international organization, on transfer of personal data has been concluded and confirmed.

In the process of ratification of an international agreement on personal data transfer, the fulfilment of the conditions referred to in Para 3 of this Article shall be specially determined.

The government shall continuously monitor developments with regard to personal data protection in a third country, parts of its territory, areas of activity, or in an international organisation, on the basis of information collected directly and taking into account information collected by international organizations, which are important for reviewing the existence of an adequate level of protection.

The list of countries, parts of their territories, areas of activity and international organizations which are considered to have provided an adequate level of protection, or for which the Government has determined that they do not provide an adequate level of protection, shall be published in the "Official Gazette of the Republic of Serbia".

Transfer with implementation of appropriate safeguards

Article 65.

The controller or processor may transfer personal data to a third country, parts of its territory, areas of activity or legal regulation, or an international organisation which is not included in the list of the government referred to in Article 64 Para 7 of this Law, only if the controller or processor has provided appropriate safeguards, and on condition that the exercise of the rights of data subjects and effective legal remedies for data subjects' rights is ensured.

The appropriate safeguards referred to in Para 1 of this Article may be provided for, without requiring any specific authorisation from the Commissioner, by:

- 1) a legally binding instrument in the relationship among public authority bodies;
- 2) the standard contractual clauses developed by the commissioner in accordance with article 45 of this law, which fully regulate a legal relationship between the controller and the processor;
- 3) binding internal corporate rules, in accordance with Article 67 of this Law;

4) an approved code of conduct pursuant to Article 59 of this Law, together with mandatory and enforceable implementation of the appropriate safeguards, including as regards data subjects' rights, by the controller or the processor in the third country;

5) issued certificates pursuant to Article 61 of this Law, together with binding and enforceable undertaken commitments of the controller or processor in the third country, to apply the appropriate safeguards, including as regards data subjects' rights.

The appropriate safeguards referred to in Para 1 of this Article may be ensured by special authorization of the Commissioner, by:

1) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation;

2) provisions of administrative arrangements between public authority bodies, which are entered into arrangement and ensure effective and enforceable legal protection of data subjects' rights.

The Commissioner shall issue authorization referred to in Para 3 of this Article within 60 days from the day of submission of the request for authorization.

The provisions of Paras 1 to 4 of this Article shall not apply to transfer of personal data processed by competent authorities for special purposes.

Transfer of data processed by competent authorities for special purposes, with
implementation of appropriate safeguards

Article 66.

Where personal data processed by competent authorities for special purposes, transfer of personal data to a third country, parts of its territory, areas of activity or legal regulation or an international organisation which is not covered by the list of the government referred in Article 64 Para 7 of this Law, shall be allowed only if:

1) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or

2) the controller has assessed all the circumstances surrounding the transfer of personal data and concluded that appropriate safeguards exist with regard to the protection of personal data.

The controller shall inform the Commissioner about transfer performed under Para 1 Item 2 of this Article.

The controller shall document a transfer performed under Para 1 Item 2 of this Article and the documentation shall be made available to the Commissioner on request.

Documentation referred to in Para 3 of this Article shall contain information on the date and time of the transfer, the receiving competent authority, the justification for the transfer and the personal data transferred.

Binding corporate rules

Article 67.

The Commissioner shall approve binding corporate rules, if they jointly meet the following conditions:

1) they are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises, including their employees;

2) expressly confer enforceable rights of data subjects with regard to the processing of their personal data; and

3) fulfil the requirements laid down in Para 2 of this Article.

Rules referred to in Para 1 of this Article shall at least regulate:

1) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members separately;

2) the data transfers or set of transfers of personal data, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country in which the data is transferred;

3) their legally binding nature, for each of the controllers separately and within a group;

4) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

5) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing and profiling in accordance with Article 38 of this Law, the right to lodge a complaint with the Commissioner and before the competent courts in accordance with Articles 82 and 84 of this Law, and to obtain compensation for a breach of these rules;

6) the acceptance by the controller or processor, with permanent residence, temporary residence, or seat in the territory of the Republic of Serbia, of liability for any breaches of the binding corporate rules by another member of the group without permanent residence, temporary residence, or seat in the territory of the Republic of Serbia, except where the controller or the processor proves that that other member of the group is not legally responsible;

7) how the information on the binding corporate rules, in particular on the provisions referred to in Items 4 to 6 of this Para is provided to the data subjects in addition to information referred to in Articles 23 and 24 of this Law;

8) the authority of data protection officer designated in accordance with Article 58 of this Law, or any other person in charge of monitoring compliance with the binding corporate rules, within the group of undertakings, or group of enterprises engaged in a joint economic activity, including monitoring over training and complaint-handling within the group;

9) the complaint procedures;

10) the monitoring mechanisms, pursuant to binding corporate rules, within the group of undertakings, or group of enterprises engaged in a joint economic activity. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in Item 8 of this Para and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the Commissioner;

11) the mechanisms for reporting and recording changes to the rules and reporting those changes to the Commissioner;

12) the cooperation mechanism with the Commissioner to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity separately, in particular the method of making available to the Commissioner the results of verifications of the measures referred to in Item 10 of this Para;

13) the mechanisms for reporting to the Commissioner on any legal requirements to which a member of the group of undertakings or group of enterprises engaged in a joint economic activity is subject to in a third country, and which are likely to have a substantial adverse effect on the safeguards provided by these rules;

14) the appropriate data protection training to personnel having permanent or regular access to personal data.

The Commissioner may specify the methods for the exchange of information between controllers, processors and the Commissioner in implementing Para 2 of this Article.

If the conditions referred to in paragraph 1 of this Article are fulfilled, the Commissioner shall issue authorization referred to in Para 2 of this Article within 60 days from the day of submission of the request for authorization.

The provisions of Paras 1 to 4 of this Article shall not apply to the transfer of data processed by competent authorities for special purposes.

Transfer or disclosure of personal data on the basis of an individual decision of an authority
of a third country

Article 68

Any decision of the court or administrative body made in a third country requiring a controller or a processor to transfer or disclose personal data may be recognised or enforceable in the territory of the Republic of Serbia, only if it is based on an international agreement, such as a mutual legal assistance treaty in force between the Republic of Serbia and that third country, without prejudice to implementation of other grounds for transfer pursuant to this Chapter of this Law.

The provisions of Para 1 of this Article shall not apply to the transfer of data processed by competent authorities for special purposes.

Transfer of personal data in specific situations

Article 69.

If a transfer of personal data is not performed in line with Articles 64, 65 and 67 of this Law, these data can be transferred to a third country or international organization, only in one of the following cases:

1) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

2) the transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken at the data subject's request;

3) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

4) the transfer is necessary for the realization of an important public interest

prescribed by the law of the Republic of Serbia and provided that this Law does not limit the transfer of certain categories of personal data;

5) the transfer is necessary for the establishment, exercise or defence of legal claims;

6) the transfer is necessary in order to protect the vital interests of the data subject or of other natural persons, under the condition that the data subject is physically incapable of giving consent or incapable of giving consent due to the lack of legal capacity; 7) specific data contained in a public register are transferred, which are available to a person who can demonstrate a legitimate interest or to the public, but only to the extent that the conditions laid down by law in relation to their availability are fulfilled.

Where transfer cannot be carried out in line with Para 1 of this Article and Articles 64, 65 and 67 of this Law, personal data may be transferred to a third country or international organization only if the following conditions are met together:

1) the transfer is performed only once and is not repetitive;

2) concerns only a limited number of data subjects;

3) is necessary for the purposes of compelling legitimate interests pursued by the controller, which are not overridden by the interests or rights and freedoms of the data subject; and

4) the controller has provided suitable safeguards and mechanisms with regard to the protection of personal data, based on prior assessment of all the circumstances surrounding the data transfer.

The controller, or the processor, is obliged to provide evidence of the performed assessment and application of the appropriate safeguards referred to in Para 2, Item 4 of this Article in the records on the processing operations referred to in Article 47 of this Law.

The controller shall notify the Commissioner on the transfer of data performed in accordance with Para 2 of this Article.

The controller shall also provide information on the transfer of data referred to in Para 2 of this Article to the data subject, along with the information prescribed in Article 23 and

24 of this Law, including information on the legitimate interests of the controller achieved by the transfer pursuant to Para 2 Item 3 of this Article.

The transfer in accordance with Para 1, Item 7 of this Article, cannot apply to all data from the registry or individual personal data category in its entirety.

Where data which are available only to the person who can demonstrate legitimate interest, are transferred from the register in accordance with Para 1, Item 7 of this Article, the data can be transferred only at the request of that person or if the person is a data recipient.

Provisions of Para 1 Items 1 to 3 and Para 2 of this Article shall not apply to activities carried out by public authorities in the exercise of their public powers.

Provisions of Paras 1 to 8 of this Article shall not apply to the transfer of data processed by competent authorities for special purposes.

Transfer of personal data processed by competent authorities for special purposes

Article 70.

Where the transfer of personal data processed by competent authorities for special purposes is not carried out pursuant to the provisions of Articles 64 and 66 of this Law, transfer of these personal data to a third country or an international organisation may take place only if the transfer is necessary in one of the following cases:

- 1) in order to protect the vital interests of the data subject or another natural person;
- 2) to safeguard legitimate interests of the data subject and where the law so provides;
- 3) for the prevention of an immediate and serious threat to public security of the Republic of Serbia or a third country;
- 4) in individual cases for special purposes;
- 5) in an individual case for the establishment, exercise or defence of legal claims relating to special purposes.

Personal data shall not be transferred if the transferring competent authority determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer set out in Para 1 Items 4 and 5 of this Article.

The competent authority shall document the transfer carried out pursuant to Para 1 of this Article and the documentation shall be made available to the Commissioner on request.

The documentation on transfer referred to in Para 3 of this Article shall contain information on the date and time of the transfer, the receiving competent authority, the justification for the transfer and the personal data transferred.

Transfer of personal data processed by competent authorities for special purposes to
the recipient in a third country

Article 71.

By way of derogation from Article 63 Para 2 Item 2 of this Law, and without prejudice to implementation of any international agreement referred to in Para 2 of this Article, the competent authority, referred to in Article 4 Item 26 sub-item a) of this Law, processing data for special purposes, may transfer personal data directly to the recipient established in the third country only if the other provisions of this Law are complied with and all of the following conditions are fulfilled:

1) the transfer is strictly necessary for the performance of a task of the transferring competent authority as provided for by law for special purposes;

2) the transferring competent authority determines that no fundamental rights and freedoms of the data subject concerned override the public interest the protection of which requires the data transfer;

3) the transferring competent authority considers that the transfer for special purposes to the competent authority established in a third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in due time;

4) the competent authority in the third country was informed of the transfer without undue delay, unless this is ineffective or inappropriate for achieving the purpose;

5) the transferring competent authority informed the recipient in the third country of the specified purpose of the personal data processing and that processing is to be performed only for that purpose, only by the recipient and only provided that such processing is necessary.

International agreement referred to in Para 1 of this Article shall apply to any international agreement concluded between the Republic of Serbia and one or more third countries in the field of judicial cooperation in criminal matters and police cooperation.

The transferring competent authority shall inform the Commissioner about transfers carried out under Para 1 of this Article.

The competent authority shall document the transfers carried out pursuant to Para 1 of this Article and the documentation shall be made available to the Commissioner on request.

The documentation on transfer referred to in Para 4 of this Article shall contain information on the date and time of the transfer, the recipient, the justification for the transfer and the personal data transferred.

International cooperation for the protection of personal data

Article 72.

The Commissioner shall take appropriate steps in relation to bodies competent for personal data protection in third countries and international organisations to:

1) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

2) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, referral to protection proceedings, legal aid in monitoring or supervision and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms of data subjects;

3) engage relevant stakeholders in activities and discussions aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data;

4) promote and improve the exchange information on personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

VI. THE COMMISSIONER

1. Independent status

Supervisory authority

Article 73.

In order to protect the fundamental rights and freedoms of natural persons in relation to processing of personal data, the tasks of monitoring over the implementation of this law in line with prescribed competences shall be performed by the Commissioner as an independent state body.

The Commissioner shall have a deputy for personal data protection.

The provision of the law governing free access to information of public importance, shall apply in relation to the seat of the Commissioner, election, termination of function, discharge procedure, position of the Commissioner, professional service, financing and submission of the reports unless this Law provides otherwise.

Independence

Article 74.

In performing its tasks and exercising its powers, in accordance with this Law, the Commissioner shall act with complete independence, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.

The Commissioner shall refrain from any action incompatible with their duties and shall not engage in any incompatible occupation, whether lucrative or not, or perform any

other public function or exercise any other public authority and shall not be a member of an association or political party or act politically.

In order to ensure the effective performance of its tasks and exercise of its powers, the necessary financial resources for work, the premises, as well as the necessary technical, organizational and staffing conditions for the work of the Commissioner shall be provided in accordance with the law governing budget and the laws regulating the state administration and the position of civil servants.

The Commissioner independently carries out the selection of employees among candidates who meet the conditions for work in state bodies prescribed by law, and manages them completely autonomously.

Supervision over the expenditure of funds for the work of the Commissioner is performed by the State Audit Institution, in accordance with the law, in a manner that does not affect the independence of the Commissioner.

Conditions for appointment of the Commissioner

Article 75.

In addition to the conditions for appointment of the Commissioner, prescribed by the law governing free access to information of public importance, the Commissioner shall have the necessary expertise and experience in the field of personal data protection.

Duty of professional secrecy

Article 76.

The Commissioner, Deputy Commissioner and staff at the Commissioner shall be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers, including information regarding breaches of this Law that was introduced to it by a person who is not employed at the Commissioner.

The obligation referred to in Para 1 of this Article shall persist after the termination of the term of office of the Commissioner, Deputy Commissioner or termination of work at the Commissioner.

2. Competences of the Commissioner

General competences

Article 77.

The Commissioner exercises its powers in the territory of the Republic of Serbia in accordance with this Law.

In exercising its powers, the Commissioner shall act in accordance with the law governing administrative procedure and the law governing inspection, if this Law does not provide otherwise.

The Commissioner is not competent to supervise processing operations of courts in the exercise of their judicial capacity.

Tasks of the Commissioner

Article 78.

The Commissioner shall:

- 1) monitor and enforce the application of this Law, in line with its competences;
- 2) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing, and in particular on processing of personal data of children;
- 3) provide opinion, in accordance with the regulations, to the National Assembly, the Government, other public authority bodies and organizations about legal and other measures related to the protection of the rights and freedoms of natural persons in relation to the processing of personal data;
- 4) promote the awareness of controllers and processors of their obligations under this Law;

5) upon request of the data subject, provide information concerning the exercise of their rights under this Law;

6) handles complaints lodged by the data subjects, investigates whether there was a breach of this Law and provides information to the applicant on the course and the results of the proceedings implemented in line with Article 82 of this Law;

7) cooperate with supervisory authorities in other states regarding personal data protection, and in particular in relation to exchange of information and provision of mutual legal assistance;

8) conduct investigations on the application of this Law in accordance with this law and the law governing inspection, and submit requests for initiating the misdemeanour proceedings when it determines that this law has been breached, in accordance with the law governing misdemeanours;

9) monitor relevant developments of information and communication technologies and commercial practices, relevant for the protection of personal data;

10) adopt standard contractual clauses referred to in Article 45 Para 11 of this Law;

11) establish and publish a list pursuant to Article 54 Para 5 of this Law;

12) provide written opinion referred to in Article 55 Para 4 of this Law;

13) keeps the record of data protection officers referred to in Article 56, paragraph 11 of this Law;

14) encourage the drawing up of codes of conduct pursuant to Article 59 Para 1 of this Law and provide an opinion and approve such codes of conduct pursuant to Article 59 Para 5 of this Law;

15) performs duties in accordance with Article 60 of this Law;

16) encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 61 Para 1 of this Law, and approve the criteria of certification pursuant to Article 61 Para 5 of this Law;

17) carry out a periodic review of certifications issued in accordance with Article 61 Para 8 of this Law;

18) prescribe and publish the criteria for accreditation of a certification body pursuant to Article 62 of this Law;

19) authorise contractual clauses and provisions referred to in Article 65 Para 3 of this Law;

20) approve binding internal corporate rules pursuant to Article 67 of this Law;

21) keep internal records of infringements of this Law and of measures taken in accordance with Article 79 Para 2 of this Law;

22) fulfil any other tasks in accordance with this Law.

The Commissioner performs the supervision activities referred to in Para 1, Item. 1) and 8) of this Article through authorized persons from the Commissioner's professional service.

The record referred to in Para 1, Item 21) of this Article shall contain: data on controllers or processors who violated this Law (their first and last name or title, place of residence, domicile, headquarters), data on violations of this Law (description of violation and article of the law violated), data on measures taken and data on the compliance of the controller or processor with the imposed measures.

The Commissioner shall prescribe the form of the record referred to in Para 3 of this Article and the manner of its keeping.

In order to simplify the submission of a complaint, the Commissioner shall prescribe a complaint submission form, which can also be completed electronically, without excluding other means of communication.

The Commissioner shall carry out its tasks in a manner that is free of charge for the data subject and data protection officer.

Where complaints are manifestly unfounded, excessive, or because of their repetitive character, the Commissioner may refuse to act on the request, along with a rationale demonstrating the manifestly unfounded, excessive or repetitive character of the request.

Investigative and other powers:

Article 79.

The Commissioner is authorized:

- 1) to order the controller and the processor, and where applicable their representatives, to provide any information it requires for the performance of its tasks;
- 2) to check and evaluate the implementation of the provisions of this Law and otherwise carry out investigations in the form of data protection audits;
- 3) to carry out a review on certifications issued pursuant to Article 61 Para 8 of this Law;
- 4) to notify the controller or the processor of an alleged infringement of this Law;
- 5) to seek and obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
- 6) to seek and obtain access to any premises of the controller and the processor, including to any data processing equipment and means utilized for personal data protection.

The Commissioner shall have all of the following corrective powers:

- 1) to issue warnings to a controller or processor by submitting written opinion that intended processing operations are likely to infringe provisions of this Law pursuant to Article 55 Para 4 of this Law;
- 2) to issue reprimands to a controller or a processor, where processing operations have infringed provisions of this Law;
- 3) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Law;
- 4) to order the controller or processor to bring processing operations into compliance with the provisions of this Law, in a specified manner and within a specified period;
- 5) to order the controller to communicate a personal data breach to the data subject;

6) to impose a temporary or definitive limitation including a ban on processing;

7) to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 29 to 32 of this Law and notification of other controllers or recipients to whom the personal data have been disclosed, pursuant to Article 30 Para 3 and Articles 33 and 34 of this Law;

8) to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 61 and 62 of this Law, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;

9) to impose an administrative fine based on a misdemeanour warrant if an inspection determined a misdemeanor for which the fine in fixed amount is prescribed by this Law, in addition to, or instead of measures prescribed by this Para, depending on the circumstances of each individual case;

10) to order the suspension of data flows to a recipient in a third country or to an international organisation.

The Commissioner is also authorized to:

1) develop standard contractual clauses referred to in Article 45 Para Article 11 of this Law;

2) to advise the controllers in the process of prior notification and obtaining opinion of the Commissioner, in line with Article 55 of this Law;

3) to issue, on its own initiative or on request, opinions to the national parliament, the Government or to other institutions and bodies, as well as to the public, on any issue related to the protection of personal data;

4) to register and publish codes of conduct it has previously approved, pursuant to Article 59 Para 5 of this Law;

5) to issue certifications and approve criteria of certification in accordance with Article 61 Para 5 of this Law;

6) to prescribe accreditation criteria pursuant to Article 62 of this Law;

7) to authorise contractual clauses, or provisions entered into agreements, in line with Article 65 Para 3 of this Law;

8) to approve binding corporate rules pursuant to Article 67 of this Law.

Supervision over the Commissioner's acts issued pursuant to this Article shall be exercised by the court in accordance with this Law.

The Commissioner may initiate a procedure before a court or other authority, in exercising the powers provided for in this Article, in accordance with the law.

Reporting on infringements of the law

Article 80.

The competent authority processing personal data for special purposes shall ensure the application of effective mechanisms for confidential reporting of cases of violation of this law to the Commissioner.

Reporting

Article 81.

The Commissioner shall draw up an annual report on its activities, with information on the types of violations of this Law and the measures taken in connection with those violations, which shall be submitted to the National Assembly.

The report referred to in Para 1 of this Article shall also be submitted to the Government, and shall be made publicly available, in an appropriate manner.

VII. LEGAL REMEDIES, LIABILITY AND SANCTIONS

The right to lodge a complaint before the Commissioner

Article 82.

The data subject shall have the right to lodge a complaint with the Commissioner, if he or she considers that the processing of his or her personal data was contrary to the

provisions of this Law. In the procedure upon complaint, the provisions of the law governing inspection are applied accordingly in the part related to the handling of complaints. Lodging a complaint with the Commissioner shall not affect the right of the data subject to otherwise engage in proceedings involving administrative or court protection.

The Commissioner shall inform the complainant about the course of procedure it performs, the results of the procedure, as well as the right of a person to initiate court proceedings in accordance with Article 83 of this Law.

Right to court protection against the decision of the Commissioner

Article 83.

The data subject, the controller, the processor, or other natural or legal person to whom the Commissioner's decision made in accordance with this Law relates to, have the right to initiate an administrative dispute against this decision within 30 days from the date of receipt of the decision. Initiation of administrative dispute shall not affect the person's right to otherwise engage in administrative or court proceedings.

If the Commissioner does not act upon a complaint within a period of 60 days from the date of submission of the complaint, or does not act in accordance with Article 82 Para 2 of this Law, the data subject has the right to initiate an administrative dispute.

Judicial protection of the rights of persons

Article 84.

The data subject shall have the right to judicial protection if he or she considers that his or her right prescribed by this Law has been infringed by the act of processing personal data on the part of the controller or processor contrary to the provisions of this Law. Submission of a lawsuit before court shall not affect the person's right to initiate other proceedings involving administrative or court protection

Submission of a lawsuit before court shall not affect the person's right to initiate other administrative or court proceedings.

The lawsuit for protection of the rights referred to in Para 1 of this Article may require the court to oblige the defendant to:

- 1) provide the information referred to in Articles 22 to 27 and Articles 33 to 35 and Article 37 of this Law;
- 2) to correct, or to delete data on the claimant referred to in Articles 29, 30 and 32 of this Law;
- 3) to limit the processing referred to in Articles 31 and 32 of this Law;
- 4) to provide data in a structured, normally used and electronically readable format;
- 5) to transfer data to another controller referred to in Article 36 of this Law;
- 6) to cease data processing referred to in Article 37 of this Law.

The lawsuit for protection of the rights referred to in Para 1 of this Article may require the court to determine that the decision concerning the data subject was made contrary to Articles 38 and 39 of this Law.

The lawsuit referred to in Paras 2 and 3 of this Article shall be submitted to the higher court on the territory where the controller or the processor or their representative, has permanent or temporary residence or seat or on the territory where the data subject has permanent or temporary residence, except if the controller or the processor is a public authority body.

The review of the final decision made upon the lawsuits referred to in Paras 2 and 3 of this Article shall always be allowed.

In the protection procedure referred to in Para 1 of this Article, the provisions of the law governing civil proceedings shall apply, unless this Law provides otherwise.

Representation of data subjects

Article 85.

Data subject has the right to authorize a representative of the association engaged in protection of rights and freedoms of data subjects, and in connection to the protection of personal data, to represent him or her in accordance with the law in the proceedings

prescribed in Articles 82 to 84 of this Law, as well as the proceedings prescribed in Article 86 of this Law.

Right to compensation

Article 86.

Any person who has suffered material or non-material damage as a result of an infringement of this Law, shall have the right to receive compensation from the controller or processor for the damage suffered.

If material or non-material damages resulted from illegal processing of data by competent authorities for special purposes, or from the breach of the provisions of the law governing processing of these data, the person who suffered damage shall have the right to compensation from the controller or other body against which a compensation claim can be brought pursuant to law.

The controller shall be liable for damages referred to in Para 1 of this Article, and a processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Law specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

A controller or processor shall be exempt from liability for damage if it proves that it is not responsible in any way for the damage.

Where more than one controller or processor, or both a controller and a processor, are processing personal data and are responsible for the damage, each controller or processor shall be held liable for the entire damage.

Where a controller or processor referred to in Para 5 of this Article has paid full compensation for the damage suffered, he or she shall be entitled to claim back from the other controllers or processors that part of the compensation corresponding to their part of responsibility for the damage, in accordance with Para 3 of this Article.

Conditions for imposing administrative fines

Article 87.

Administrative fines for infringements of the provisions of this Law in each individual case shall be imposed and implemented in effective, proportionate and dissuasive manner.

Administrative fines referred to in Para 1 of this Article shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in Article 79 Para 2 Items 1 to 8 and Item 10 of this Law.

When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case, the Commissioner shall give due regard to the following:

1) the nature, gravity and duration of the infringement, taking into account the nature, scope, or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage suffered by them;

2) the intentional or negligent character of the infringement;

3) any action taken by the controller or processor to remove or mitigate the damage suffered by data subjects;

4) the degree of responsibility of the controller and processor, taking into account the measures implemented by them pursuant to Articles 42 and 50 of this Law;

5) previous infringements of the provisions of this Law by the controller or processor, which are relevant for prescribing the sanction;

6) the degree of cooperation of the controller or processor with the Commissioner, in order to remedy the infringement and remove or mitigate the possible adverse effects of the infringement;

7) the categories of personal data affected by the infringement;

8) the manner in which the infringement became known to the Commissioner, in particular whether, and if so, to what extent, the controller or processor notified the Commissioner of the infringement;

9) compliance with the corrective measures of the Commissioner which have previously been ordered against the controller or processor concerned with regard to the same subject-matter, in line with Article 79 Para 2 of this Law;

10) implementation of approved codes of conduct pursuant to Article 59 of this Law, or issued certificates pursuant to Article 61 of this Law;

11) any other aggravating or mitigating factors applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement of the provisions of this Law.

VIII.SPECIFIC PROCESSING SITUATIONS

Processing and freedom of expression and information

Article 88.

For processing carried out for journalistic purposes and publishing in the media, or the purpose of academic, artistic or literary expression, provisions of the Chapter II to VI and Articles 89 to 94 of this Law, shall not apply, if and to the extent to which, in the concrete case, this limitation is necessary for the protection of the freedom of expression and information.

Personal data processing and access to information of public importance

Article 89.

Information of public importance which include personal data can be made available to the applicant by the public authority body in a manner that ensures that the right of the public to know and the right to personal data protection can be achieved together, to the extent provided by law governing free access to information of public importance and this Law.

Processing of a unique registration number of citizens

Article 90.

For processing of a unique registration number of citizens, the provisions of the law governing the unique registration number of citizens or other law shall apply, along with the provisions of this law relating to the protection of the rights and freedoms of the data subjects.

Processing in the field of labour and employment,

Article 91.

For personal data protection in the field of labor and employment, provisions of the law governing labor and employment, as well as collective agreement, shall be implemented along with the provisions of this Law.

If the collective agreement contains provisions on protection of personal data, safeguards of personal dignity legitimate interests and fundamental rights of data subjects shall be prescribed, and in particular taking into account transparency of processing, exchange of personal data within the group of undertakings engaged in a joint economic activity, as well as the monitoring system at the workplace.

Safeguards and limitations of implementation of the provisions of the law for data processing relating to archiving in public interest, scientific or historical research and statistical purposes

Article 92.

The processing of personal data for the purposes of archiving in the public interest, scientific or historical research and for statistical purposes shall be subject to the appropriate mechanisms safeguarding the rights and freedoms of the data subjects prescribed by this Law. These mechanisms shall ensure implementation of appropriate technical, organizational and staffing measures and in particular for the purpose of the application of the principle of minimization of personal data. These measures may include data pseudonymization, provided that the purpose can be achieved by applying this measure.

If the purpose referred to in Para 1 of this Article can be achieved without the identification of the data subject, or without further identification of the data subject, the purpose must be achieved in that manner, or the processing must be carried out in a manner that does not allow the identification of the data subject.

Provisions on the rights of data subjects referred to in Articles 26, 29, and Articles 31 to 37 of this Law shall not apply in cases where the processing of personal data is performed for the purpose of scientific or historical research, or for statistical purposes, if this is necessary for the achievement of these purposes, or if the application of these provisions

would prevent or significantly hinder their realization, with the application of the measures referred to in Paras 1 and 2 of this Article.

Provisions on the rights of data subjects referred to in Articles 26 and 29 and articles 31 to 37 of this Law shall not apply in cases where personal data processing is performed for the purpose of archiving in the public interest, if this is necessary for the achievement of this purpose, or if the application of these provisions would prevent or significantly hinder its realization, with the application of the measures referred to in Paras 1 and 2 of this Article.

If processing referred to in Paras 3 and 4 of this Article is performed for other purposes, processing of such other purposes shall be subject to the provisions of this law without restriction.

Personal data processing by churches and religious communities

Article 93.

If personal data processing is regulated by special rules of the church or religious community, these rules must be aligned with the provisions of this law.

In the case referred to in Para 1 of this Article, the provisions of this Law on the inspection and other competences and authority of the Commissioner from Articles 77 to 79 of this Law shall also apply, unless a church or religious community establishes a special independent supervisory body which will exercise such authority, provided that such a body meets the conditions prescribed in Chapter VI of this Law.

Processing personal data for humanitarian purposes by public authority bodies

Article 94.

Personal data processed by a public authority may also be processed for the purpose of collecting funds for humanitarian purposes, with the application of appropriate safeguards for the protection of the rights and freedoms of data subjects, in accordance with this Law.

For the purpose of collecting funds for humanitarian purposes, personal data processed by a public authority cannot be transferred to third parties.

X. PENAL PROVISIONS

Article 95.

The controller or the processor having the status of a legal entity shall be fined for a misdemeanour from RSD 50,000 to 2,000,000RSD if he:

- 1) processes personal data contrary to the principles of processing referred to in Article 5, Para 1 of this Law;
- 2) processes personal data for other purposes, contrary to Art. 6 and 7 of this Law;
- 3) does not clearly separate personal data which are based on facts from personal data based on personal assessment (Article 10);
- 4) by using reasonable measures, does not ensure that incorrect, incomplete and outdated personal data are transferred, or that they are available (Article 11, Para 1);
- 5) processes personal data, without consent of the data subject and is not able to indicate that the data subject has consented to the processing of his data (Article 15, Para 1);
- 6) processes specific personal data contrary to Art. 17 and 18 of this Law;
- 7) processes personal data relating to criminal judgments, criminal offences and security measures contrary to Article 19 Para 1 of this Law;
- 8) does not provide the information referred to in Article 23, Paras 1 to 3 and Article 24 paras 1 to 4 of this Law to the data subject;
- 9) does not make available or does not provide information to the data subject contrary to Article 25 of this Law;
- 10) fails to provide the information requested, does not provide access to information, or does not provide a copy of the data processed (Article 26 paras 1 and 2 and Article 27);
- 11) limits the right of the data subject, partially or fully, to access the data relating to him or her, contrary to Article 28 Para 1 of this Law;
- 12) does not correct incorrect data or does not supplement incomplete data contrary to Article 29 of this Law;
- 13) does not delete the data of the person to whom the data relate without delay in the cases referred to in Article 30 Para 2 of this Law;
- 14) does not limit the processing of personal data in cases referred to in Article 31 of this Law;

- 15) does not delete personal data (Article 32);
- 16) fails to notify the recipient regarding the rectification, erasure and restriction of processing (Article 33, Para 1);
- 17) fails to inform the data subject of the decision on refusal to rectify, erase or restrict processing, as well as the reason for refusal (Article 34, Para 1);
- 18) does not interrupt the processing of data after the data subject filed an objection to such processing (Article 37, para 1);
- 19) a decision is made which produces legal consequences for the data subject solely on the basis of automated processing, contrary to Articles 38 and 39 of this Law;
- 20) when determining the method of processing, as well as during the processing, does not undertake appropriate organizational, staffing and technical measures contrary to Article 42 of this Law;
- 21) the relationship between joint controllers is not regulated in a legally prescribed manner in line with Article 43 Paras 2 to 5 of this law;
- 22) entrusts processing of personal data to the processor, contrary to Article 45 of this Law;
- 23) data is processed without or contrary to the order of the controller (Article 46);
- 24) fails to notify the Commissioner of data security violation, contrary to Article 52 of this Law;
- 25) fails to notify the data subject of the data security breach, contrary to Article 53 of this Law;
- 26) fails to assess the impact on the protection of data security in the manner provided for in Article 54 of this Law;
- 27) fails to notify the Commissioner, or does not seek the opinion of the Commissioner prior to the commencement of the processing operation (Article 55, Paras 1 and 3);
- 28) does not appoint a data protection officer in cases referred to in Article 56, Para 2 of this Law;
- 29) does not perform its obligations towards the data protection officer referred to in Article 57 Paras 1 to 3 of this Law;
- 30) the transfer of personal data to third countries and international organizations is carried out contrary to Articles 63 to 71 of this Law;

31) does not ensure the implementation of effective mechanisms for confidential reporting of cases of violation of this law (Article 80);

32) processes personal data for purposes of archiving in the public interest, scientific or historical research, or for statistical purposes contrary to Article 92 of this Law.

The controller or the processor who has attributes of the legal entity shall be fined in the amount of 100,000rsd if:

1) does not inform the recipient about the special conditions for the processing of personal data prescribed by law and its obligation to comply with these conditions (article 11, para 5);

2) do not submit to the data subject the reasoned decision or does not notify him or her in the deadline stipulated in Article 28 Paras 3 and 5 of this Law;

3) continues processing for the purposes of direct marketing and the data subject objected to such processing (Article 37, Para 3);

4) does not designate its representative in the Republic of Serbia, contrary to Article 44 of this Law;

5) does not keep the prescribed provisional records (Article 47), or does not record processing actions (Article 48);

6) does not publish the contact details of the data protection officer and do not submit them to the Commissioner (Article 56, Para 11).

A natural person who does not keep as a professional secret the personal data he or she has learned during the performance of his duties shall be punished for a misdemeanour with a fine of 5,000 RSD to 150,000 RSD; (Article 57 Para 7 and Article 76);

For misdemeanour referred to in Para 1 of this Article, an entrepreneur shall be fined between 20,000RSD and 500,000RSD.

For the misdemeanour referred to in Para 1 of this Article, a natural person, that is, a responsible person in a legal entity, a state authority, or a territorial autonomy authority and in a local self-government unit, as well as a responsible person in a representative office or a business unit of a foreign legal entity shall be fined from 5,000RSD to 150,000RSD.

For the misdemeanour referred to in Para 2 of this Article an entrepreneur shall be fined 50.000 RSD.

For the misdemeanour referred to in Para 2 of this Article a natural person, that is, a responsible person in a legal entity, a state authority, or a territorial autonomy authority and in a local self-government unit, as well as a responsible person in a representative office or a business unit of a foreign legal entity shall be fined in amount of 20,000rsd.

X. TRANSITIONAL AND FINAL PROVISIONS

Deputy Commissioner

Article 96.

Deputy Commissioner elected pursuant to the Law on Personal Data Protection ("Official Gazette of the Republic of Serbia" No. 97/08, 104/09 – oth.law, 68/12 – CC and 107/12), shall continue to perform its duty until the expiration of the mandate for which he was elected.

Initiated proceedings

Article 97.

Complaints procedures regarding the requests for exercising the rights related to processing, procedures of transfer of data from the Republic of Serbia and monitoring procedures which have not been completed by the date of start of implementation of this Law, shall be terminated according to the provisions of the Law on Personal Data Protection ("Official Gazette of the Republic of Serbia" No. 97/08, 104/09 – oth.law, 68/12 – CC and 107/12).

Central Registry of Databases

Article 98.

The Central Registry of Databases established under the provisions of the Law on Personal Data Protection ("Official Gazette of the Republic of Serbia" No. 97/08, 104/09 – oth.law, 68/12 – CC and 107/12) shall cease to be kept on the day of entry into force of this Law.

The Central Registry referred to in Para 1 of this Article, as well as the data contained in that register, shall be treated in accordance with the regulations governing the treatment of archives.

Bylaws

Article 99.

The bylaws envisaged by this Law shall be adopted within nine months from the date of entry into force of this Law.

By-laws issued on the basis of the Law on Personal Data Protection ("Official Gazette of the Republic of Serbia" No. 97/08, 104/09 – oth.law, 68/12 – CC and 107/12) shall continue to apply until the adoption of bylaws referred to in para 1 of this Article, if they are not in contravention of this Law.

Harmonization of other laws

Article 100.

Provisions of other laws which refer to processing of personal data shall be aligned with the provisions of this Law by the end of 2020.

Termination of the validity of the previous law

Article 101.

On the day of entry into force of this law, Law on Personal Data Protection ("Official Gazette of the Republic of Serbia" No. 97/08, 104/09 – oth.law, 68/12 – CC and 107/12) shall cease to apply.

Entry into force

Article 102.

This law shall enter into force on the eighth day from the date of its publication in the "Official Gazette of the Republic of Serbia", and shall apply after the expiration of nine months from the date of entry into force, except the provisions of Article 98 of this Law, which shall be applied from the day of entry into force of this Law.