

**PERSONAL DATA PROTECTION ACT OF THE  
REPUBLIC OF SLOVENIA**

Ministry of Justice of the Republic of Slovenia

2004

---

---

**MINISTRY OF JUSTICE OF SLOVENIA LEGISLATION SERIES, NO. 8**

**Disclaimer:** The English language translation of the text of the Personal Data Protection Act (of the Republic of Slovenia) below is provided just for information only and confers no rights nor imposes any obligations on anyone. Only the official publication of the Personal Data Protection Act in Slovene language, as published and promulgated in the Official Gazette of the Republic of Slovenia, is authentic. The status of the translated text of the Personal Data Protection Act is as of 17 October 2005 and the status of statutes and other information in footnotes and in Appendixes is also as of 17 October 2005. The explanatory footnotes and appendices have also been inserted just for information only, and previous text of this Disclaimer also applies to them. While the Government Translation Service prepared the original translation, Ministry of Justice of the Republic of Slovenia performed the substantially corrected translation, terminology decisions and annotations. This translation may not be published in any way, without the prior permission of the Ministry of Justice of the Republic of Slovenia, but may be used for information purposes only. Further editorial revisions of this translation are possible.

---

On the basis of the second indent, first paragraph of Article 107 and the first paragraph of Article 91 of the Constitution of the Republic of Slovenia, I hereby issue the

**DECREE**

**on the promulgation of the Personal Data Protection Act (ZVOP-1)**

I hereby promulgate the Personal Data Protection Act (ZVOP-1), which was adopted by the National Assembly of the Republic of Slovenia at its session of 15 July 2004.

No. 001-22-148/04  
Ljubljana, 23 July 2004

Dr. Janez Drnovšek  
President  
of the Republic of Slovenia

## **PERSONAL DATA PROTECTION ACT (ZVOP-1)<sup>1</sup>**

### **PART I GENERAL PROVISIONS**

#### **Contents of the Act**

##### Article 1

This Act determines the rights, responsibilities, principles and measures to prevent unconstitutional, unlawful<sup>2</sup> and unjustified encroachments on the privacy and dignity of an individual<sup>3</sup> (hereinafter: individual) in the processing of personal data.

#### **Principle of lawfulness and fairness**

##### Article 2

Personal data shall be processed lawfully<sup>4</sup> and fairly.

#### **Principle of proportionality**

##### Article 3

Personal data that are being processed must be adequate and in their extent appropriate in relation to the purposes for which they are collected and further processed.

#### **Prohibition of discrimination**

##### Article 4

Protection of personal data shall be guaranteed to every individual irrespective of nationality<sup>5</sup>, race, colour, religious belief, ethnicity, sex, language, political or other belief, sexual orientation, material standing, birth, education, social position, citizenship, place or type of residence or any other personal circumstance.

---

<sup>1</sup> Personal Data Protection Act is in Slovene language: Zakon o varstvu osebnih podatkov. ZVOP-1 is its official acronym in Slovene language. This Act was published in: Official Gazette of the Republic of Slovenia, No. 86/2004, as of 5 August 2004.

<sup>2</sup> A verbatim translation would be: "not in accordance with the statute".

<sup>3</sup> In original text of this Act in Slovene language the term "individual" is used both in its male and female form ("posameznik oziroma posameznica").

<sup>4</sup> A verbatim translation would be: "statutorily" - meaning by the statute/following a statute (a general act of Parliament).

<sup>5</sup> Citizenship.

## **Territorial application of this Act**

### Article 5

- (1) This Act shall apply to the processing of personal data if the data controller is established, has its seat or is registered in the Republic of Slovenia, or if a subsidiary of the data controller is registered in the Republic of Slovenia.
- (2) This Act shall also apply if the data controller is not established, does not have its seat or is not registered in a Member State of the European Union or is not a part of the European Economic Area and for the processing of personal data the data controller uses automated or other equipment located in the Republic of Slovenia, except where such equipment is used solely for the transfer of personal data across the territory of the Republic of Slovenia.
- (3) The data controller from the previous paragraph must appoint a natural person or legal person that has its seat or is registered in the Republic of Slovenia to represent it in respect of the processing of personal data in accordance with this Act.
- (4) This Act shall also apply to diplomatic-consular offices and other official representative offices of the Republic of Slovenia abroad.

## **Meaning of terms**

### Article 6

Terms used in this Act shall have the following meanings:

1. Personal data - is any data relating to an individual, irrespective of the form in which it is expressed.
2. Individual - is an identified or identifiable natural person to whom personal data relates; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity, where the method of identification does not incur large costs or disproportionate effort or require a large amount of time.
3. Processing of personal data - means any operation or set of operations performed in connection with personal data that are subject to automated processing or which in manual processing are part of a filing system or which are intended for inclusion in a filing system, such as in particular collection, acquisition, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, communication, dissemination or otherwise making available, alignment or linking, blocking, anonymising, erasure or destruction; processing may be performed manually or by using automated technology (means of processing).
4. Automated processing – is the processing of personal data using information technology means.

5. Filing system – is any structured set of data containing at least one piece of personal data, which is accessible according to criteria enabling the use or combination of the data, irrespective of whether the set is centralised, decentralised or dispersed on a functional or geographical basis; a structured set of data is a set of data organised in such a manner as to identify or enable identification of an individual.

6. Data controller - is a natural person or legal person or other public or private sector person which alone or jointly with others determines the purposes and means of the processing of personal data or a person provided by statute that also determines the purposes and means of processing.

7. Data processor - is a natural person or legal person that processes personal data on behalf and for the account of the data controller.

8. Data recipient – is a natural or legal person or other private or public sector person to whom personal data are supplied or disclosed.

9. Supply of personal data – is the supply or disclosure of personal data.

10. Foreign recipient and foreign data controller – is a recipient of personal data in a third country and a data controller in a third country.

11. Third country - is a country that is not a Member State of the European Union or a part of the European Economic Area.

12. Filing system catalogue - is a description of a filing system.

13. Register of Filing Systems - is a register containing data from filing system catalogues.

14. Personal consent of an individual – is a voluntary statement of the will of an individual that his personal data may be processed for a specific purpose, and this is given on the basis of information that must be provided to such individual by the data controller pursuant to this Act; personal consent of an individual may be written, oral or some other appropriate consent of the individual.

15. Written consent of the individual - is the signed consent of the individual having the form of a document, the provision of a contract, the provision of an order, an appendix to an application or other form in accordance with statute; a signature shall also mean on the basis of a statute a form equivalent to a signature given by means of telecommunication and a form equivalent by statute to a signature given by an individual who does not know how to write or is unable to write.

16. Oral or other appropriate consent of the individual - is consent given orally or by means of telecommunication or other appropriate means or in some other appropriate manner from which it can be concluded unambiguously that the individual has given his consent.

17. Blocking - is such labelling of personal data that restricts or prevents their further processing.

18. Anonymising - is such alteration to the form of personal data such that they can no longer be linked to the individual or where such link can only be made with disproportionate efforts, expense or use of time.

19. Sensitive personal data - are data on racial, national or ethnic origin, political, religious or philosophical beliefs, trade-union membership, health status, sexual life, the entry in or removal from criminal record or records of minor offences that are kept on the basis of a statute that regulates minor offences (hereinafter: minor offence records); biometric characteristics are also sensitive personal data if their use makes it possible to identify an individual in connection with any of the aforementioned circumstances.

20. Same connecting codes - are the personal identification number and other uniform identification numbers defined by statute relating to an individual that can be used to obtain or retrieve personal data from filing systems in which the same connecting codes are also processed.

21. Biometric characteristics - are such physical, physiological and behavioural characteristics which all individuals have but which are unique and permanent for each individual specifically and which can be used to identify an individual, in particular by the use of fingerprint, recording of papillary ridges of the finger, iris scan, retinal scan, recording of facial characteristics<sup>6</sup>, recording of an ear, DNA scan and characteristic gait.

22. Public sector - are state bodies, bodies of self-governing local communities, holders of public powers, public agencies, public funds, public institutes, universities, independent institutions of higher education and self-governing communities of nationalities.

23. Private sector - means legal or natural persons performing an activity in accordance with the statute regulating commercial companies or a commercial public service or craft, and persons of private law; public commercial institutes, public companies and commercial companies, irrespective of the share or influence held by the state, self-governing local communities or self-governing communities of nationalities, are a part of the private sector.

### **Exceptions in the application of this Act**

#### *Article 7*

(1) This Act shall not apply to the processing of personal data performed by individuals exclusively for personal use, family life or for other domestic needs.

(2) Articles 26, 27 and 28 of this Act shall not apply to personal data, which are processed by political parties, trade unions, associations or religious communities relating to their members.

(3) The second paragraph of Article 25, Articles 26, 27 and 28, and Part V of this Act shall not apply to personal data which are processed by the media for the purposes of informing the public.

---

<sup>6</sup> A verbatim translation of the term "obraz" (in Slovene language) would be: "face".

## **PART II**

### **PROCESSING OF PERSONAL DATA**

#### **Chapter 1**

##### **Legal grounds and purposes**

###### **General definition**

###### Article 8

(1) Personal data may only be processed if the processing of personal data and the personal data being processed are provided by statute, or if the personal consent of the individual has been given for the processing of certain personal data.

(2) The purpose of processing personal data must be provided by statute, and in cases of processing on the basis of personal consent of the individual, the individual must be informed in advance in writing or in another appropriate manner of the purpose of processing of personal data.

###### **Legal grounds in the public sector**

###### Article 9

(1) Personal data in the public sector may be processed if the processing of personal data and the personal data being processed are provided by statute. Statute may provide that certain personal data may only be processed on the basis of personal consent of the individual.

(2) Holders of public powers may also process personal data on the basis of personal consent of the individual without statutory grounds where this does not involve the performance of their duties as holders of public powers. Filing systems created on such basis must be held separate from filing systems created on the basis of the performance of duties of the holder of public powers.

(3) Irrespective of the first paragraph of this Article, in the public sector personal data may be processed in respect of individuals that have contractual relations with the public sector or on the basis of the individual's initiative are negotiating on the conclusion of a contract, provided that the processing of personal data is necessary and appropriate for conducting negotiations for the conclusion of a contract or for the fulfilment of a contract.

(4) Irrespective of the first paragraph of this Article, personal data may in exceptions be processed in the public sector where they are essential for the exercise of lawful<sup>7</sup> competences, duties or obligations by the public sector, provided that such processing does not encroach on the justified interests of the individual to whom the personal data relate.

---

<sup>7</sup> Provided for by statute (a general act of Parliament).

## **Legal grounds in the private sector**

### Article 10

- (1) Personal data in the private sector may be processed if the processing of personal data and the personal data being processed are provided by statute, or if the personal consent of the individual has been given for the processing of certain personal data.
- (2) Irrespective of the previous paragraph, in the private sector personal data may be processed in respect of individuals that have contractual relations with the private sector or on the basis of the individual's initiative are negotiating on the conclusion of a contract, provided that the processing of personal data is necessary and appropriate for conducting negotiations for the conclusion of a contract or for the fulfilment of a contract.
- (3) Irrespective of the first paragraph of this Article, personal data may be processed in the private sector if this is essential for the fulfilment of the lawful<sup>8</sup> interests of the private sector and these interests clearly outweigh the interests of the individual to whom the personal data relate.

## **Contractual Processing**

### Article 11

- (1) Data controller may by contract entrust individual tasks related to processing of personal data to data processor that is registered to perform such activities and ensures the appropriate procedures and measures pursuant to Article 24 of this Act.
- (2) Data processor may perform individual tasks associated with processing of personal data within the scope of the client's authorisations, and may not process personal data for any other purpose. Mutual rights and obligations shall be arranged by contract, which must be concluded in writing and must also contain an agreement on the procedures and measures pursuant to Article 24 of this Act. Data controller shall oversee the implementation of procedures and measures pursuant to Article 24 of this Act.
- (3) In the event of a dispute between the data controller and the data processor, the data processor shall be bound on the basis of a request from the data controller to return to the controller without delay the personal data processed under contract. He shall be obliged to destroy immediately or to supply any copies of such data to the state body competent by statute for detection or prosecution of criminal offences, to a court or to another state body, if so provided by statute.
- (4) In the event of cessation of a data processor, personal data shall be returned to the data controller without unnecessary delay.

---

<sup>8</sup> Provided for by statute (a general act of Parliament).

## Protection of the vital interests of the individual

### Article 12

If processing of personal data is necessarily required to protect the life or body of an individual, his personal data may be processed irrespective of the fact that there are no other statutory legal grounds for the processing of such data.

## Processing of sensitive personal data

### Article 13

Sensitive personal data may only be processed in the following cases:

1. if the individual has given explicit personal consent for this, such consent as a rule being in writing, and in the public sector provided by statute;
2. if the processing is necessary in order to fulfil the obligations and special rights of a data controller in the area of employment in accordance with statute, which also provides appropriate guarantees for the rights of the individual;
3. if the processing is necessarily required to protect the life or body of an individual to whom the personal data relate, or of another person, where the individual to whom the personal data relate is physically or contractually<sup>9</sup> incapable of giving his consent pursuant to subparagraph 1 of this Article;
4. if they are processed for the purposes of lawful<sup>10</sup> activities by institutions, societies, associations, religious communities, trade unions or other non-profit organisations with political, philosophical, religious or trade-union aim, but only if the processing concerns their members or individuals in regular contact with them in connection with such aims, and if they do not supply such data to other individuals or persons of public or private sector without the written consent of the individual to whom they relate;
5. if the individual to whom the sensitive personal data relate publicly announces them without any evident or explicit purpose of restricting their use;
6. if they are processed by health-care workers and health-care staff in compliance with statute for the purposes of protecting the health of the public and individuals and the management or operation of health services;

---

<sup>9</sup> This term "contractually" represents the abbreviation of the Slovene legal institute of "capacity to contract" (for the purposes of this Act), which is in Slovene "poslovna sposobnost". For example, a similar German legal term is "*Geschäftsfähigkeit*". In the Republic of Slovenia natural persons obtain the **partial capacity to contract** when they attain 15 years of age (see Article 108 of the Marriage and Family Relations Act, Official Gazette of the SRS, Nos. 15/76, 30/86, 1/89 and 14/89 – consolidated text, Official Gazette of the RS, Nos. 13/94, 82/94, 29/95, 26/99, 60/99 – Decision of the Constitutional Court, 70/2000, 64/2001, 110/2002, 16/2004 and 69/2004 - officially consolidated text) and obtain the **full capacity to contract** when they attain 18 years of age (Article 117, paragraph 1 of the Marriage and Family Relations Act), or if a minor (a person between 15 years and below 18 years of age) under certain conditions concludes a marital union (Article 117, paragraph 2) and a minor can also obtain it if he/she became a parent and if there are "significant" reasons for obtaining the full capacity to contract (Article 117, paragraph 3), following a decision by the court in non-contentious proceedings.

<sup>10</sup> Provided for by statute (a general act of Parliament).

7. if this is necessary in order to assert or oppose a legal claim;
8. if so provided by another statute in order to implement the public interest.

### **Protection of sensitive personal data**

#### Article 14

(1) Sensitive personal data must during processing be specially marked and protected, such that access to them by unauthorised persons is prevented, except in instances from subparagraph 5 of Article 13 of this Act.

(2) In the transmission of sensitive personal data over telecommunications networks, data shall be considered as suitably protected if they are sent with the use of cryptographic methods and electronic signatures such that their illegibility or non-recognition is ensured during transmission.

### **Automated decision-making**

#### Article 15

Automated data processing, in which a decision may be taken regarding an individual that could have legal effect in relation to him, or substantive influence on him, and which is based solely on automated data processing intended for the evaluation of certain personal aspects relating to him, such as in particular his success at work, credit rating, reliability, handling or compliance with conditions required, shall only be permitted if the decision:

1. is taken during the conclusion or implementation of a contract, provided that the request to conclude or implement a contract submitted by the individual to whom the personal data relate has been fulfilled or that there exist appropriate measures to protect his lawful<sup>11</sup> interests, such as in particular agreements enabling him to object to such decision or to express his position;
2. is provided by statute which also provides measures to protect the lawful<sup>12</sup> interests of the individual to whom the personal data relate, particularly the possibility of legal remedy against such decision.

### **Purpose of collection, and further processing**

#### Article 16

Personal data may only be collected for specific and lawful<sup>13</sup> purposes, and may not be further processed in such a manner that their processing would be counter to these purposes, unless otherwise provided by statute.

---

<sup>11</sup> Provided for by statute (a general act of Parliament).

<sup>12</sup> Provided for by statute (a general act of Parliament).

<sup>13</sup> Provided for by statute (a general act of Parliament).

## **Processing for historical, statistical and scientific-research purposes**

### Article 17

- (1) Irrespective of the initial purpose of collection, personal data may be further processed for historical, statistical and scientific-research purposes.
- (2) Personal data shall be supplied to the data recipient for the purpose of processing from the previous paragraph in an anonymised form, unless otherwise provided by statute or if the individual to whom the personal data relate gave prior written consent for the data to be processed without anonymising.
- (3) Personal data supplied to data recipient in accordance with the previous paragraph shall on completion of processing be destroyed, unless otherwise provided by statute. The data recipient shall be obliged without delay after destruction of the data to inform the data controller who supplied him the personal data in writing when and how he destroyed them.
- (4) Results of processing from the first paragraph of this Article shall be published in anonymised form, unless otherwise provided by statute or unless the individual to whom the personal data relate gave written consent for publication in a non-anonymised form or unless written consent for such publication has been given by the heirs to the deceased person under this Act.

## **Chapter 2**

### **Protection of individuals**

#### **Accuracy and up to date personal data**

### Article 18

- (1) Personal data being processed must be accurate and kept up to date.
- (2) Data controller may prior to input into a filing system verify the accuracy of personal data by examining an identity document or other suitable public document of the individual to whom the data relate.

#### **Informing the individual of the processing of personal data**

### Article 19

- (1) If personal data are collected directly from the individual to whom they relate, the data controller or his representative must communicate to the individual the following information, if the individual is not yet acquainted with them:
  - data on the data controller and his possible representative (personal name, title or official name respectively and address or seat respectively),
  - the purpose of the processing of personal data.

(2) If in view of the special circumstances of collecting personal data from the previous paragraph there is a need to ensure lawful<sup>14</sup> and fair processing of personal data of the individual, the person from the previous paragraph must also communicate to the individual the additional information, if the individual is not yet acquainted with them, and in particular:

- a declaration as to the data recipient or the type of data recipients of his personal data,
- a declaration of whether the collection of personal data is compulsory or voluntary, and the possible consequences if the individual will not provide data voluntarily,
- information on the right to consult, transcribe, copy, supplement, correct, block and erase personal data that relate to him.

(3) If personal data were not collected directly from the individual to whom they relate, the data controller or his representative must communicate to the individual the following information no later than on the recording or supply of personal data to the data recipient:

- data on the data controller and his possible representative (personal name, title or official name respectively and address or seat respectively),
- the purpose of the processing of personal data.

(4) If in view of the special circumstances of collecting personal data from the previous paragraph there is a need to ensure lawful<sup>15</sup> and fair processing of personal data of the individual, the person from the previous paragraph must also communicate to the individual additional information, and in particular:

- information on the type of personal data collected,
- a declaration as to the data recipient or the type of data recipients of his personal data,
- information on the right to consult, transcribe, copy, supplement, correct, block and erase personal data that relate to him.

(5) Information from the third and fourth paragraphs of this Article shall not need to be ensured if in order to process personal data for historical, statistical or scientific-research purposes it would be impossible or would incur large costs or disproportionate effort or would require a large amount of time, or if the recording or supply of personal data is expressly provided by statute.

### **Use of the same connecting code**

#### Article 20

(1) In the acquisition of personal data from filing systems in the areas of health, police, national intelligence-security activities, national defence, judiciary and the state prosecution and criminal record and minor offence records, the same connecting code may not be used in such manner that only such code would be used to obtain personal data.

(2) Irrespective of the previous paragraph, the same connecting code may exceptionally be used to obtain personal data if this is the only item of data in a specific case that can enable the detection or prosecution of a criminal offence *ex officio*, to protect the life or body of an individual, or to ensure the implementation of the tasks of the intelligence and security bodies provided by statute. An official annotation or other written record must be made thereof without delay.

---

<sup>14</sup> Verbatim: statutory (in accordance with a statute, meaning mostly in accordance with this Act).

<sup>15</sup> Verbatim: statutory (in accordance with a statute, meaning mostly in accordance with this Act).

(3) The first paragraph of this Article shall not apply to the land register and the commercial register.

### **Duration of storage of personal data**

#### Article 21

(1) Personal data may only be stored for as long as necessary to achieve the purpose for which they were collected or further processed.

(2) On completion of the purpose of processing, personal data shall be erased, destroyed, blocked or anonymised, unless pursuant to the statute governing archive materials and archives they are defined as archive material, or unless a statute otherwise provides for an individual type of personal data.

### **Supply of personal data**

#### Article 22

(1) Data controllers shall be obliged against payment of the cost of supply, unless otherwise provided by statute, to supply personal data to data recipients.

(2) The data controller of the Central Population Register or of Records of Permanently and Temporarily Registered Residents shall be obliged in the manner defined for the issuing of certificates to supply to authorised party demonstrating a lawful interest in exercising rights before public sector persons the personal name and address of permanent or temporary residence of an individual against whom they are exercising their rights.

(3) Data controller shall be obliged for each supply of personal data to ensure that it is subsequently possible to determine which personal data were supplied, to whom, when and on what basis, for the period covered by statutory protection of the rights of an individual due to non-allowed supply of personal data.

(4) Irrespective of the first paragraph of this Article, data controllers in the public sector shall be bound to supply to data recipient in the public sector personal data without payment of the cost of supply, unless otherwise provided by statute or unless it involves use for historical, statistical or scientific-research purposes.

### **Protection of personal data of deceased individuals**

#### Article 23

(1) Data controller may supply data on a deceased individual only to those data recipients authorised to process personal data by statute.

(2) Irrespective of the previous paragraph, data controller shall supply data on a deceased individual to the person who under the statute governing inheritance is the deceased person's legal heir of the first or second order, if they demonstrate a lawful interest in the use of

personal data and the deceased individual did not prohibit in writing the supply of such personal data.

(3) Unless otherwise provided by statute, a data controller may also supply data from the previous paragraph to any other person intending to use such data for historical, statistical or scientific-research purposes if the deceased individual did not prohibit in writing the supply of such personal data.

(4) If the deceased individual did not issue a prohibition from the previous paragraph, persons who under the statute governing inheritance are his legal heirs of the first or second order may prohibit in writing the supply of his data, unless otherwise provided by statute.

### **Chapter 3**

#### **Security of Personal Data**

##### **Contents**

##### Article 24

(1) Security of personal data comprises organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data:

1. by protecting premises, equipment and systems software, including input-output units;
2. by protecting software applications used to process personal data;
3. by preventing unauthorised access to personal data during transmission thereof, including transmission via telecommunications means and networks;
4. by ensuring effective methods of blocking, destruction, deletion or anonymisation of personal data;
5. by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.

(2) In cases of processing of personal data accessible over telecommunications means or network, the hardware, systems software and software applications must ensure that the processing of personal data in filing systems is within the limits of authorisations of the data recipient.

(3) The procedures and measures to protect personal data must be adequate in view of the risk posed by processing and the nature of the specific personal data being processed.

(4) Functionaries, employees and other individuals performing work or tasks at persons that process personal data shall be bound to protect the secrecy of personal data with which they become familiar in performing their functions, work and tasks. The duty to protect the secrecy

of personal data shall also be binding on them after termination of their function, work or tasks, or the performance of contractual processing services.

### **Duty to secure**

#### Article 25

(1) Data controllers and data processors shall be bound to ensure the protection of personal data in the manner set out in Article 24 of this Act.

(2) Data controllers shall prescribe in their internal acts the procedures and measures for security of personal data and shall define the persons responsible for individual filing systems and the persons who, due to the nature of their work, shall process individual personal data.

### **Chapter 4**

#### **Notification of filing systems**

##### **Filing system catalogue**

#### Article 26

(1) Data controller shall establish for each filing system a filing system catalogue containing:

1. title of the filing system;
2. data on the data controller (for natural person: personal name, address where activities are performed or address of permanent or temporary residence, and for sole trader his official name, registered office, seat and registration number; for legal person: title or registered office and address or seat of the data controller and registration number);
3. legal basis for processing personal data;
4. the category of individuals to whom the personal data relate;
5. the type of personal data in the filing system;
6. purpose of processing;
7. duration of storage of personal data;
8. restrictions on the rights of individuals with regard to personal data in the filing system and the legal basis for such restrictions;
9. data recipients or categories of data recipients of personal data contained in the filing system;
10. whether the personal data are transferred to a third country, to where, to whom and the legal grounds for such transfer;

11. a general description of security of personal data;
  12. data on linked filing systems from official records and public books.
  13. data on the representative from the third paragraph of Article 5 of this Act (for natural person: personal name, address where activities are performed or address of permanent or temporary residence, and for sole trader his official name, registered office, seat and registration number; for legal person: title or registered office and address or seat of the data controller and registration number).
- (2) Data controller must ensure that the contents of the catalogue are accurate and up to date.

### **Notification of the supervisory body**

#### Article 27

- (1) Data controller shall supply data from subparagraphs 1, 2, 4, 5, 6, 9, 10, 11, 12 and 13 of the first paragraph of Article 26 of this Act to the National Supervisory Body for Personal Data Protection at least 15 days prior to the establishing of a filing system or prior to the entry of a new type of personal data.
- (2) Data controller shall supply to the National Supervisory Body for Personal Data Protection modifications to the data from the previous paragraph no later than eight days from the date of modification.
- (3) Data from the first paragraph of this Article shall not need to be supplied by that data controller that do not have more than 20 persons employed for an indefinite period and relating to those filing systems they maintain on their employees in accordance with the statute governing filing systems in the area of labour. In this case each person must be provided with information from Article 26 of this Act.

### **Register**

#### Article 28

- (1) The National Supervisory Body for Personal Data Protection shall manage and maintain a Register of Filing Systems containing data from Article 27 of this Act, in the manner defined by the methodology of its management.
- (2) The Register shall be managed using information technology and shall be published on the website of the National Supervisory Body for Personal Data Protection (hereinafter: the website).
- (3) The rules on the methodology<sup>16</sup> from the first paragraph of this Article shall be defined by the Minister responsible for justice, on the proposal of the Chief National Supervisor for Personal Data Protection<sup>17</sup> (hereinafter: the Chief National Supervisor).

---

<sup>16</sup> See: Rules on the Methodology of Managing the Register of Filing Systems (Official Gazette of the RS, No. 28/2005).

### **PART III**

#### **RIGHTS OF THE INDIVIDUAL**

##### **Examination of the Register**

###### Article 29

(1) The National Supervisory Body for Personal Data Protection shall be obliged to permit anyone to consult the Register of Filing Systems and to transcribe the data.

(2) The consultation and transcription of data must as a rule be permitted and enabled on the same day, and no later than within eight days, otherwise the request shall be deemed to have been refused.

##### **Right of the individual to information**

###### Article 30

(1) Data controller shall on request of the individual be obliged:

1. to enable consultation of the filing system catalogue;
2. to certify whether data relating to him are being processed or not, and to enable him to consult personal data contained in filing system that relate to him, and to transcribe or copy them;
3. to supply him an extract of personal data contained in filing system that relate to him;
4. to provide a list of data recipients to whom personal data were supplied, when, on what basis and for what purpose;
5. to provide information on the sources on which records contained about the individual in a filing system are based, and on the method of processing.
6. to provide information on the purpose of processing and the type of personal data being processed, and all necessary explanations in this connection;
7. to explain technical and logical-technical procedures of decision-making, if the controller is performing automated decision-making through the processing of personal data of an individual.

(2) The extract from subparagraph 3 of the previous paragraph may not replace the document or certificate under the regulations on administrative or other procedures, and this shall be indicated on the extract.

---

<sup>17</sup> In original text of this Act in Slovene language the term "the Chief National Supervisor for Protection of Personal Data" is used both in its female and male form ("glavna državna nadzornica oziroma glavni državni nadzornik za varstvo osebnih podatkov").

### **Procedure for information**

#### Article 31

- (1) The request from Article 30 of this Act shall be lodged in writing or orally in an annotation with the data controller. Such request may be lodged once every three months, and in respect of personal data under the provisions of Chapter 2, Part VI of this Act, once a month.
- (2) The data controller must enable the individual to consult, transcribe, copy and obtain a certificate pursuant to subparagraphs 1 and 2 of the first paragraph of Article 30 of this Act no later than 15 days from the date of receipt of the request, or within the same interval to inform the individual in writing of the reasons why he will not enable consultation, transcription, copying or the issuing of a certificate.
- (3) The data controller shall be obliged to supply the extract from subparagraph 3, the list from subparagraph 4, information from subparagraphs 5 and 6 and the explanation from subparagraph 7 of the first paragraph of Article 30 of this Act to the individual within 30 days from the date he received the request, or within the same interval to inform him in writing of the reasons why he will not supply the extract, list, information or explanation.
- (4) If the data controller fails to act in accordance with the second and third paragraphs of this Article, the request shall be deemed to have been refused.
- (5) Costs relating to the request and consultation from this Article shall be borne by the data controller.

### **Right to supplement, correct, block, erase and to object**

#### Article 32

- (1) On the request of an individual to whom personal data relate, the data controller must supplement, correct, block or erase personal data which the individual proves as being incomplete, inaccurate or not up to date, or that they were collected or processed contrary to statute.
- (2) On the request of the individual the data controller must inform all data recipients and data processors to whom the controller has supplied the personal data of the individual, before the measures from the previous paragraph have been carried out, of their supplementation, correction, blocking or erasure pursuant to the previous paragraph. Exceptionally the data controller shall not need to do this if it would incur large costs, disproportionate efforts or would require a large amount of time.
- (3) Individuals whose personal data are processed in accordance with the fourth paragraph of Article 9 or the third paragraph of Article 10 of this Act shall have the right through objection at any time to demand the cessation of their processing. The data controller shall grant the objection if the individual demonstrates that the conditions for processing have not been fulfilled pursuant to the fourth paragraph of Article 9 or the third paragraph of Article 10 of this Act. In this case the personal data of the individual may no longer be processed.

(4) If the data controller does not grant the objection from the previous paragraph, the individual that lodged the objection may request that the National Supervisory Body for Personal Data Protection decides on whether the processing is in accordance with the fourth paragraph of Article 9 or the third paragraph of Article 10 of this Act. The individual may lodge such request within seven days of delivery of the decision regarding on objection.

(5) The National Supervisory Body for Personal Data Protection shall decide on the request from the previous paragraph within two months of receipt of the request. The lodging of a request shall withhold the processing of personal data of the individual in respect of which the request was lodged.

(6) The costs of all actions of the data controller from the previous paragraphs shall be borne by the data controller.

### **Procedure of supplementing, correction, blocking, deletion and objection**

#### Article 33

(1) The request or objection from Article 32 of this Act shall be lodged in writing or orally in an annotation with the data controller.

(2) The data controller shall be obliged to perform the supplementing, correction, blocking or deletion of personal data within 15 days of the date of receipt of the request, and to inform the person who lodged the request thereof, or within the same interval to inform him of the reasons why he will not do so. The controller must decide on an objection within the same deadline.

(3) If the data controller fails to act pursuant to the previous paragraph, the request shall be deemed to have been refused.

(4) If the data controller concludes on his own that the personal data are incomplete, inaccurate or not up to date, he shall supplement or correct them and inform the individual thereof, unless otherwise provided by statute.

(5) Costs relating to the supplementing, correction and erasure of personal data, and of the notification and decision on the objection, shall be borne by the data controller.

### **Judicial protection of the rights of the individual**

#### Article 34

(1) Individual who finds that his rights provided by this Act have been violated may request judicial protection for as long as such violation lasts.

(2) If the violation from the previous paragraph ceases, the individual may file a suit to rule that the violation existed if he is not provided with other judicial protection in relation to the violation.

(3) The competent court shall decide in the procedure under the provisions of the statute regulating administrative disputes unless otherwise provided by this Act.

(4) The procedure shall not be public unless the court decides otherwise at the suggestion of the individual for well-founded reasons.

(5) The procedure shall be urgent and a priority.

### **Temporary injunction**

#### Article 35

In a suit filed due to violations of rights from Article 32 of this Act, an individual may request the court to bind the data controller, until a final decision is issued in the administrative dispute, to prevent any kind of processing of the disputed personal data, if their processing could cause with difficulty reparable damage to the individual, to whom the personal data relate, while the postponement of processing should not be contrary to the public interests and neither is there any danger of greater irredeemable damage being done to the opposing party.

### **Restriction of the rights of an individual**

#### Article 36

(1) The rights of an individual from the third and fourth paragraphs of Article 19, Articles 30 and 32 of this Act may exceptionally be restricted by statute for reasons of protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state, the exercise of the responsibilities of the police, the prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or tax reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others.

(2) Restrictions from the previous paragraph may only be provided in the extent necessary to achieve the purpose for which the restriction was provided.

## **PART IV**

### **INSTITUTIONAL PERSONAL DATA PROTECTION**

#### **Chapter 1**

#### **Supervisory body for personal data protection**

#### **Supervisory body**

#### Article 37

(1) The National Supervisory Body for Personal Data Protection (hereinafter: the National Supervisory Body) shall have the status of supervisory body for the protection of personal data.

(2) The National Supervisory Body shall undertake inspection supervision on the implementation of the provisions of this Act and other tasks under this Act and other regulations regulating the protection or processing of personal data or the transfer of personal data from the Republic of Slovenia. The National Supervisory Body shall also undertake other tasks in accordance with statute.

(3) The National Supervisory Body shall ensure uniform realisation of measures in the area of protection of personal data.

### **Status and organisation of the National Supervisory Body**

#### Article 38

(1) The National Supervisory Body shall be a self-dependent<sup>18</sup> state body.

(2) The National Supervisory Body shall be headed by a Chief National Supervisor, who shall be a state functionary. His salary shall be regulated by the decision of the National Assembly laying down the ranking of official functions into salary brackets.

(3) The National Supervisory Body shall employ at least four National Supervisors for Personal Data Protection<sup>19</sup> (hereinafter: the Supervisor). At least one of them must be a university graduate in law.

(4) The Chief National Supervisor shall head and represent the National Supervisory Body, organise and coordinate the work of Supervisors and carry out inspection supervision pursuant to this Act.

(5) Administrative and technical tasks for the National Supervisory Body shall be performed by the Ministry responsible for justice.

### **Funds for the work of the National Supervisory Body**

#### Article 39

Funds for the work of the National Supervisory Body shall be provided in the Budget of the Republic of Slovenia. The level of funds shall be determined by the National Assembly of the Republic of Slovenia (hereinafter: National Assembly) on the proposal of the Chief National Supervisor.

---

<sup>18</sup> In Slovene language "self-dependent" is: "samostojen". A literal translation would be: "standing on its own". Self-dependent means from the viewpoint of legal terminology less than independent and more than autonomy. A similar legal term in German language is "*Selbständigkeit*". However, in actual terms self-dependent is understood to mean the same as independent.

<sup>19</sup> In original text of this Act in Slovene language the term "National Supervisors for Personal Data Protection" is used in its female and male form ("državna nadzornica oziroma državni nadzornik za varstvo osebnih podatkov").

### **Appointment of the Chief National Supervisor**

#### Article 40

- (1) The Chief National Supervisor shall be appointed by the National Assembly on the proposal of the Minister responsible for justice.
- (2) The Chief National Supervisor shall be appointed from among those individuals that fulfil the conditions for appointment to the title of Supervisor under this Act.
- (3) The vacancy for the post of Chief National Supervisor shall be advertised by the Ministry responsible for justice *ex officio* no later than three months from the expiry of the term of office of the Chief National Supervisor or within one month of early dismissal. The vacancy shall be advertised in the Official Gazette of the Republic of Slovenia, and the deadline for applications may not be shorter than 15 days.
- (4) The Chief National Supervisor shall be appointed for a period of eight years and may be re-appointed.

### **Dismissal of the Chief National Supervisor**

#### Article 41

- (1) The Chief National Supervisor may be subject to early dismissal only in the following cases:
  - if he tenders a statement of resignation to the National Assembly;
  - if he is convicted by a final decision of a criminal offence with a punishment of deprivation of liberty;
  - if he cannot perform his function for health or other well-founded reasons for more than six months;
  - if he becomes permanently incapable of performing his function.
- (2) The Chief National Supervisor shall be dismissed early and his term of office shall cease on the day the National Assembly determines the onset of reasons from the previous paragraph.

### **Deputising for the Chief National Supervisor**

#### Article 42

The Chief National Supervisor shall from among the Supervisors appoint his Deputy, who shall deputise for him during his absence or temporary incapacity.

### **The Supervisor**

#### Article 43

- (1) Persons that have university education, five years of working experience, of which at least one year has been in work with personal data, and have passed the professional examination

for the position of inspector pursuant to the statute governing inspection supervision, may be appointed as Supervisor.

(2) Supervisors shall have the status, rights and obligations provided for Inspectors by the statute governing inspection supervision and by the statute governing civil servants, unless otherwise provided by this Act.

(3) Supervisors shall be appointed by the Chief National Supervisor in accordance with the statute governing civil servants.

### **Self-dependence of Supervisors**

#### Article 44

(1) In the performance of tasks of inspection supervision and other tasks under this Act within the framework of their authorisations, Supervisors shall be independent and shall undertake them within the framework of and on the basis of the Constitution and statutes.

(2) In relation to the performance of tasks not comprising the performance of inspection supervision, they shall be bound by the written instructions of the Chief National Supervisor.

### **Employment and assignment in the National Supervisory Body**

#### Article 45

(1) The Chief National Supervisor shall define in accordance with the statute governing civil servants in the act on systematisation the internal organisation of the National Supervisory Body and the required number of civil servants of the National Supervisory Body performing legal tasks and the required number of civil servants performing ancillary work.

(2) Civil servants of state bodies may on the basis of a proposal of the Chief National Supervisor and with their written agreement and the consent of the head of their state body be assigned to perform legal tasks or ancillary work from the previous paragraph at the National Supervisory Body for a period of up to three years. Judges, State Prosecutors and Assistant State Prosecutors may be assigned to perform such tasks pursuant to the provisions of statutes regulating the judicial service and the state prosecutor's office.

(3) Servants and functionaries from the previous paragraph may not perform the tasks of inspection supervision.

## **Chapter 2**

### **Tasks of the National Supervisory Body**

#### **Reports of the National Supervisory Body**

##### Article 46

(1) The National Supervisory Body shall submit an Annual Report on its work to the National Assembly no later than by 31 May for the previous year, and shall publish this Report on its website.

(2) The Annual Report shall contain data on the work of the National Supervisory Body in the previous year and assessments and recommendations in the area of protection of personal data.

#### **Cooperation with other bodies**

##### Article 47

The National Supervisory Body shall in its work cooperate with state bodies, the competent bodies of the European Union for the protection of individuals in the processing of personal data, international organisations, foreign supervisory bodies for the protection of personal data, institutes, societies, nongovernmental organisations in the area of protection of personal data or privacy and other organisations and bodies regarding all issues important for the protection of personal data.

#### **Competences regarding regulations**

##### Article 48

(1) The National Supervisory Body shall issue prior opinions to Ministries, the National Assembly, self-governing local community bodies, other state bodies and holders of public powers regarding the compliance of the provisions of draft statutes and other regulations with the statutes and other regulations regulating personal data.

(2) The National Supervisory Body may file a request to the Constitutional Court of the Republic of Slovenia (hereinafter: the Constitutional Court) to assess the constitutionality of statutes, other regulations and general acts issued to exercise public powers if the question of constitutionality and lawfulness arises in connection with a procedure it conducts.

#### **Publicity concerning work**

##### Article 49

(1) The National Supervisory Body may:

1. issue an internal journal and professional literature;

2. on the website or in another appropriate manner publish the prior opinion from the first paragraph of Article 48 of this Act, after the statute or other regulation has been adopted and published in the Official Gazette of the Republic of Slovenia, in the journal of a self-governing local community or publish it in another lawful<sup>20</sup> manner;
  3. on the website or in another appropriate manner publish requests from the second paragraph of Article 48 of this Act, after the Constitutional Court has received them;
  4. on the website or in another appropriate manner publish decisions and rulings of the Constitutional Court on requests from the second paragraph of Article 48 of this Act;
  5. on its website or in another appropriate manner publish decisions and rulings of courts of general jurisdiction and the Administrative Court relating to the protection of personal data, such that it is not possible to read from them the personal data of parties, injured parties, witnesses or experts;
  6. issue non-binding opinions on the compliance of codes of professional ethics, general terms of business or drafts thereof with regulations in the area of the protection of personal data;
  7. issue non-binding opinions, clarifications and positions on issues in the area of protection of personal data, and publish them on the website or in another appropriate manner;
  8. prepare and issue non-binding instructions and recommendations regarding protection of personal data in individual fields;
  9. issue public statements on inspection supervision undertaken in individual cases;
  10. hold media conferences relating to the work of the National Supervisory Body and publish transcripts of statements or recordings of statements from media conferences on the website;
  11. publish other important announcements on its website.
- (2) The National Supervisory Body may for the performance of competences from subparagraphs 6, 7 and 8 of the previous paragraph call for cooperation from representatives of associations and other nongovernmental organisations in the area of protection of personal data, privacy and consumers.

### **Chapter 3**

#### **Inspection supervision**

##### **Application of the statute governing inspection supervision**

###### Article 50

For the performance of inspection supervision under this Act, the provisions of the statute governing inspection supervision shall apply, unless otherwise provided by this Act.

---

<sup>20</sup> Verbatim: statutory (in accordance with a statute).

### **Scope of inspection supervision**

#### Article 51

Within the framework of inspection supervision the National Supervisory Body shall:

1. supervise the lawfulness<sup>21</sup> of processing of personal data;
2. supervise the suitability of measures for security of personal data and the implementation of procedures and measures for security of personal data pursuant to Articles 24 and 25 of this Act;
3. supervise the implementation of the provisions of the statute regulating the filing system catalogue, the Register of Filing Systems and the recording of the supply of personal data to individual data recipients;
4. supervise the implementation of the statutory provisions regarding the transfer of personal data to third countries and on the supply thereof to foreign data recipients.

### **Direct performance of inspection supervision**

#### Article 52

- (1) Inspection supervision shall be performed directly by Supervisors within the limits of competence of the National Supervisory Body.
- (2) Supervisor shall demonstrate his authorisation to perform the tasks of inspection supervision with an official identity card, which shall contain a photograph of the Supervisor, his personal name, professional or scientific title and other necessary data. The Minister responsible for justice shall prescribe the form and content of the official identity card in detail.

### **Competences of the Supervisor**

#### Article 53

In performing inspection supervision, the Supervisor shall be entitled:

1. to examine documentation relating to the processing of personal data, irrespective of their confidentiality or secrecy, and the transfer of personal data to third countries and the supply to foreign data recipients;
2. to examine the contents of filing systems, irrespective of their confidentiality or secrecy, and filing system catalogues;
3. to examine documentation and acts regulating the security of personal data;
4. to examine premises in which personal data are processed, computer and other equipment, and technical documentation;

---

<sup>21</sup> Verbatim: statutory compliance (in accordance with a statute).

5. to verify measures and procedures to secure personal data, and the implementation thereof;
6. to exercise other competences provided by the statute regulating inspection supervision and the statute regulating the general administrative procedure;
7. to perform other matters provided by statute.

### **Inspection measures**

#### Article 54

(1) The Supervisor who in performing inspection supervision detects a violation of this Act or of another statute or regulation regulating protection of personal data shall have the right immediately:

1. to order the elimination of irregularities or deficiencies he detects in the manner and within the interval he himself defines;
2. to order the prohibition of processing of personal data by persons in the public or private sector who have failed to ensure or failed to implement measures and procedures to secure personal data;
3. to order the prohibition of processing of personal data and the anonymising, blocking, erasure or destruction of personal data whenever he concludes that the personal data are being processed in contravention of the statutory provisions;
4. to order the prohibition of the transfer of personal data to third countries, or their supply to foreign data recipients, if they are transferred or supplied in contravention of the statutory provisions or binding international treaty;
5. to order other measures provided by the statute regulating inspection supervision and the statute regulating the general administrative procedure.

(2) Measures from the previous paragraph may not be ordered against a person who is performing in the electronic communications network services of data transfer, including temporary storage of data and other operations in connection with data which are mainly or entirely in the function of performing or facilitating the transfer of data over networks, if that person himself has no interest linked to the content of such data, and this is not a person who may himself or together with a limited circle of persons linked to him effectively control access to such data.<sup>22</sup>

(3) If a supervisor determines during inspection supervision that there exists a suspicion of the commission of a criminal offence or minor offence, he shall file a criminal notification or implement a procedure in accordance with the statute regulating minor offences.

---

<sup>22</sup> For a possible interpretation of Article 54, paragraph 2 of the Personal Data Protection Act of the Republic of Slovenia see: Bostjan Makarovic: The new Slovenian personal data protection act: Statutory limits to injunctive regulation of the internet, Computer & Security Law Report (2005), 21, Elsevier Ltd., pp. 322-327, especially pp. 326-327.

### **Judicial protection**

#### Article 55

There shall be no appeal against a decision or ruling of the Supervisor from the first paragraph of Article 54 of this Act, but an administrative dispute shall be permitted.

### **Notification to complainant**

#### Article 56

The Supervisor shall be obliged to notify complainant of all important conclusions and actions in the procedure of inspection supervision.

### **Competences of the National Supervisory Body regarding access to information of a public character**

#### Article 57

(1) The National Supervisory Body may initiate an administrative dispute against a decision of the Commissioner for Access to Information of a Public Character<sup>23</sup>, if it assesses that such decision has violated the protection of personal data.

(2) The administrative dispute procedure from the previous paragraph shall be urgent and a priority.

(3) The National Supervisory Body shall be bound to deliver to the Commissioner for Access to Information of a Public Character a decision or ruling in which the Supervisor has taken a position regarding the issue of information of a public character.

### **Protection of secrecy**

#### Article 58

(1) The Supervisor shall be obliged to protect the secrecy of personal data he encounters in performing inspection supervision, and also after ceasing to perform the Supervisor's service.

(2) The obligation from the previous paragraph shall also apply to all civil servants at the National Supervisory Body.

---

<sup>23</sup> See Act on Access to Information of a Public Character (Official Gazette of the RS, Nos. 24/03 and 61/05). In Slovene language: "Zakon o dostopu do informacij javnega značaja".

## **Chapter 4**

### **Cooperation and external supervision in the area of personal data protection**

#### **The Human Rights Ombudsman**

##### Article 59

(1) The Human Rights Ombudsman<sup>24</sup> (hereinafter: the Ombudsman) shall perform his tasks in the area of personal data protection in relation to state bodies, self-governing local community bodies and holders of public powers in accordance with the statute regulating the Human Rights Ombudsman.

(2) Personal data protection shall be a special area of the Ombudsman for which one of the Deputy Ombudsmen shall be responsible.

#### **The Annual Report**

##### Article 60

The Ombudsman shall report in his Annual Report to the National Assembly on conclusions, proposals and recommendations, and on the situation in the area of personal data protection.

#### **Competence of the National Assembly**

##### Article 61

The competent working body of the National Assembly shall monitor the situation in the area of personal data protection and the implementation of the provisions of this Act.

## **PART V**

### **TRANSFER OF PERSONAL DATA**

#### **Chapter 1**

#### **Transfer of personal data to Member States of the European Union and the European Economic Area**

##### **Free flow of personal data**

##### Article 62

Whenever personal data are supplied to data controller, data processor or data recipient established, has its seat or is registered in a Member State of the European Union or the European Economic Area or otherwise subject to the legal order thereof, the provisions of this Act on the transfer of personal data to third countries shall not apply.

---

<sup>24</sup> In original text of this Act in Slovene language the term "the Human Rights Ombudsman" is used both in its female and male form ("varuhinja oziroma varuh človekovih pravic").

## **Chapter 2**

### **Transfer of personal data to third countries**

#### **General provision**

##### Article 63

- (1) The supply of personal data that are processed or will be processed only after being supplied to a third country, shall be permitted in accordance with the provisions of this Act and provided that the National Supervisory Body issues a decision that the country to which the data are transferred ensures an adequate level of protection of personal data.
- (2) The decision from the previous paragraph shall not be required if the third country is on the list of those countries from Article 66 of this Act that have been found to fully ensure an adequate level of protection of personal data.
- (3) The decision from the first paragraph of this Article shall not be required if the third country is on the list of those countries from Article 66 of this Act that have been found in part to ensure an adequate level of protection of personal data, if those personal data are transferred and for those purposes for which an adequate level of protection has been found.

#### **Procedure for determining an adequate level of protection of personal data**

##### Article 64

- (1) The National Supervisory Body shall initiate a procedure to determine an adequate level of protection of personal data in a third country on the basis of a conclusion of inspection supervision or at the suggestion of a natural person or legal person who can show a legal interest in the issuing of a decision.
- (2) At the request of the National Supervisory Body, the Ministry responsible for foreign affairs shall obtain from the competent body of a third country the necessary information as to whether such country ensures an adequate level of protection of personal data.
- (3) The National Supervisory Body may obtain additional information on the adequate level of protection of personal data in a third country directly from other supervisory bodies and the competent body of the European Union.
- (4) The National Supervisory Body shall issue a decision within two months of receipt of full information from the second and third paragraphs of this Article. It may also issue a decision only for a certain type of personal data or for their processing for an individual purpose.
- (5) The National Supervisory Body shall be obliged no later than within 15 days of the issuing of a decision that a third country fails to ensure an adequate level of protection of personal data to inform the competent body of the European Union in writing.

## **Judicial protection**

### Article 65

There shall be no appeal against a decision from the fourth paragraph of Article 64 of this Act, but an administrative dispute shall be permitted.

## **List**

### Article 66

(1) The National Supervisory Body shall maintain a list of third countries for which it finds that have fully or partly ensured an adequate level of protection of personal data, or have not ensured such protection. If it has been determined that a third country only partly ensures an adequate level of protection of personal data, the list shall also set out in which part an adequate level has been ensured.

(2) The Chief National Supervisor shall publish the list from the previous paragraph in the Official Gazette of the Republic of Slovenia.

## **Binding of National Supervisory Body in decision-making**

### Article 67

The National Supervisory Body shall in its decision-making be bound by the decisions of the competent body of the European Union with regard to assessment as to whether third countries ensure an adequate level of protection of personal data.

## **Decision-making on the transfer of personal data**

### Article 68

(1) In decision-making on the adequate level of protection of personal data in a third country, the National Supervisory Body shall be bound to determine all circumstances relating to the transfer of personal data. In particular, it shall be obliged to take account of the type of personal data, the purpose and duration of proposed processing, the legal arrangements in the country of origin and the recipient country, including arrangements for protection of personal data of foreign citizens, and measures to secure personal data used in such countries.

(2) In decision-making from the previous paragraph, the National Supervisory Body shall in particular take account of:

1. whether the transferred personal data are used solely for the purpose for which they were transferred, or whether the purpose may change only on the basis of permission of the data controller supplying the data or on the basis of personal consent of the individual to whom the personal data relate;

2. whether the individual to whom personal data relate has the possibility of determining the purpose for which his personal data have been used, to whom they were supplied and the

possibility of correcting or erasing inaccurate or outdated personal data, unless this is prevented due to the secrecy of the procedure by binding international treaties;

3. whether the foreign data controller performs adequate organisational and technical procedures and measures to protect personal data;

4. whether there is an assigned contact person authorised to provide information to the individual to whom the personal data relate, or to the National Supervisory Body on the processing of personal data transferred;

5. whether the foreign data recipient may transfer personal data only on the condition that another foreign data recipient to whom personal data will be supplied ensures adequate protection of personal data also for foreign citizens;

6. whether effective legal protection is ensured for individuals whose personal data were transferred.

### **Rules**

#### Article 69

Following a proposal of the Chief National Supervisor, the Minister responsible for justice, with the consent of the Minister responsible for foreign affairs, shall issue rules that define in greater detail the information considered necessary in the decision-making of the National Supervisory Body on the transfer of personal data to third countries<sup>25</sup>.

### **Special provisions**

#### Article 70

(1) Irrespective of the first paragraph of Article 63 of this Act, personal data may be transferred and supplied to a third country, if:

1. so provided by another statute or binding international treaty;
2. the individual to whom the personal data relate gives personal consent and is aware of the consequences of such supply;
3. the transfer is necessary for the fulfilment of a contract between the individual to whom the personal data relate and the data controller, or for the implementation of pre-contractual measures adopted in response to the request of the individual to whom the personal data relate;
4. the transfer is necessary for the conclusion or implementation of a contract to the benefit of the individual to whom the personal data relate, concluded between the data controller and a third party;
5. the transfer is necessary in order to protect from serious danger the life or body of an individual to whom the personal data relate;

---

<sup>25</sup> See: Rules on Acquiring Required Information for the Decision-making on the Transfer of Personal Data to Third Countries (Official Gazette of the RS, No. 79/2005).

6. the transfer is performed from registers, public books or official records which are intended by statute to provide information to the public and which are available for consultation by the general public or to any person who demonstrates a legal interest that in the individual case the conditions provided by statute for consultation have been met;

7. the data controller ensures adequate measures of protection of personal data and of the fundamental rights and freedoms of individuals, and declares the possibility of their fulfilment or protection, especially in the provisions of contracts or in the general terms of business.

(2) In the case of transfer of personal data under subparagraph 7 of the previous paragraph, the person intending to transfer personal data must obtain a special decision from the National Supervisory Body permitting the transfer of personal data.

(3) The person may transfer personal data only upon receipt of the decision from the previous paragraph permitting transfer.

(4) There shall be no appeal against a decision from the second paragraph of this Article, but an administrative dispute shall be permitted. The administrative dispute procedure shall be urgent and a priority.

(5) The National Supervisory Body shall be obliged no later than within 15 days of the issuing of a decision from the second paragraph of this Article to communicate it to the competent body of the European Union and to the Member States of the European Union.

(6) If the competent body of the European Union decides upon receipt of a decision that the transfer on the basis of a decision from the second paragraph of this Article is not permissible, the National Supervisory Body shall be bound by that body's decision, and shall be obliged within five days of receipt of such decision to issue to the person from the second paragraph of this Article a new decision prohibiting him from making further transfer of personal data.

### **Recording of a transfer**

#### Article 71

The transfer of personal data to a third country shall be recorded in accordance with the provisions of subparagraph 10 of the first paragraph of Article 26 of this Act.

## **PART VI**

### **SECTORAL ARRANGEMENTS**

#### **Chapter 1**

##### **Direct marketing**

##### **Rights and responsibilities of controller**

###### Article 72

(1) Data controller may use the personal data of individuals that he obtained from publicly accessible sources or within the framework of the lawful<sup>26</sup> performance of activities, also for the purposes of offering goods, services, employment or temporary performance of work through the use of postal services, telephone calls, electronic mail or other telecommunications means (hereinafter: direct marketing<sup>27</sup>) in accordance with the provisions of this Chapter, unless otherwise provided by another statute.

(2) For the purposes of direct marketing, data controller may use only the following personal data collected in accordance with the previous paragraph: personal name, address of permanent or temporary residence, telephone number, e-mail address and fax number. On the basis of personal consent of the individual, data controller may also process other personal data, but may only process sensitive personal data if he possesses the personal consent of an individual, that is explicit and as a rule in writing.

(3) Data controller must perform direct marketing in such a way that upon the performance of direct marketing the individual is informed of his rights from Article 73 of this Act.

(4) If a data controller intends to supply personal data from the second paragraph of this Article to other data recipients for the purposes of direct marketing or to data processors, he shall be bound to inform the individual of this and prior to the supply of personal data obtain the individual's written consent. The notification to the individual regarding the intended supply must contain information as to the data intended to be supplied, to whom, and for what purpose. The costs of notification shall be borne by the data controller.

##### **Rights of individual**

###### Article 73

(1) Individual may at any time in writing or in another agreed manner request that the data controller permanently or temporarily cease to use his personal data for the purpose of direct marketing. The data controller shall be obliged within 15 days to prevent as appropriate the

---

<sup>26</sup> Verbatim: statutory (in accordance with a statute).

<sup>27</sup> The definition of direct marketing is therefore: "Data controller's use the personal data of individuals that he obtained from publicly accessible sources or within the framework of the lawful performance of activities, also for the purposes of offering goods, services, employment or temporary performance of work through the use of postal services, telephone calls, electronic mail or other telecommunications means."

use of personal data for the purpose of direct marketing, and within the subsequent 5 days to inform in writing or another agreed manner the individual who so requested.

(2) The costs of all actions of the data controller in relation to request from the previous paragraph shall be borne by the controller.

## **Chapter 2**

### **Video surveillance**

#### **General provisions**

##### Article 74

(1) The provisions of this Chapter shall apply to the implementation of video surveillance, unless otherwise provided by another statute.

(2) A public or private sector person that conducts video surveillance must publish a notice to that effect. Such notice must be visible and plainly made public in a manner that enables individuals to acquaint themselves about its implementation at the latest when the video surveillance of them begins.

(3) The notice from the previous paragraph must contain the following information:

1. that video surveillance is taking place;
2. the title of the person in the public or private sector implementing it;
3. a telephone number to obtain information as to where and for which period recordings from the video surveillance system are stored.

(4) Through notification from the second paragraph of this Article the individual shall be deemed to have been informed of the processing of personal data pursuant to Article 19 of this Act.

(5) The video surveillance system used to conduct video surveillance must be protected against access by unauthorised persons.

#### **Access to official office premises and business premises**

##### Article 75

(1) The public and private sector may implement video surveillance of access to their official office premises or business premises if necessary for the security of people or property, for ensuring supervision of entering to or exiting from their official or business premises, or where due to the nature of the work there exists a potential threat to employees. The decision shall be taken by the competent functionary, head, director or other competent or authorised individual of the person in the public sector or person in the private sector. The written decision must explain the reasons for the introduction of video surveillance. The introduction of video surveillance may also be laid down by statute or a regulation issued pursuant thereto.

(2) Video surveillance may only be implemented in a manner that does not show recordings of the interior of residential buildings that do not affect entrance to their premises, or recordings of entrances to apartments.

(3) All employees of the person in the public or private sector working in the premises under surveillance must be informed in writing of the implementation of video surveillance.

(4) The filing system under this Article shall contain a recording of the individual (an image or sound), and the date and time of entry to and exit from the premises, it may also contain the personal name of the recorded individual, the address of his permanent or temporary residence, employment, the number and data on the type of his personal document, and the reason for entry, if the personal data listed are collected in addition to or through the recording of the video surveillance system.

(5) Personal data from the previous paragraph may be stored for a maximum of one year from their creation, and shall then be erased, unless otherwise provided for by statute.

### **Apartment buildings**

#### Article 76

(1) The written consent of joint owners with a share of more than 70% of the ownership shall be required for the introduction of video surveillance in an apartment building.

(2) Video surveillance may only be introduced in an apartment building when necessary for the security of people and property.

(3) Video surveillance in apartment buildings may only monitor access to entrances and exits and common areas of apartment buildings. Video surveillance of the housekeeper's apartment and the workshop for the housekeeper shall be prohibited.

(4) It shall be prohibited to enable or implement current or subsequent examination of recordings of video surveillance systems through internal cable television, public cable television, the Internet or the use of other telecommunications means able to transmit such recordings.

(5) Entrances to individual apartments may not be recorded by video surveillance systems.

### **Work areas**

#### Article 77

(1) Video surveillance within work areas may only be implemented in exceptional cases when necessarily required for the safety of people or property or to protect secret data and business secrets, and where such purpose cannot be achieved by milder means.

(2) Video surveillance may only be implemented for those parts of areas where the interests from the previous paragraph must be protected.

- (3) Video surveillance shall be prohibited in work areas outside of the workplace, particularly in changing rooms, lifts and sanitary areas.
- (4) Employees must be informed in advance in writing prior to the commencement of implementation of video surveillance.
- (5) Prior to the introduction of video surveillance in a person of the public or private sector, the employer shall be obliged to consult the representative trade union at the employer.
- (6) In the area of national defence, national intelligence-security activities and the protection of secret data, the fourth and fifth paragraphs of this Article shall not apply.

### **Chapter 3**

#### **Biometrics**

##### **General provision**

###### Article 78

The properties of an individual shall be determined or compared through the processing of biometric characteristics so as to identify him or confirm his identity (hereinafter: biometric measures) under the conditions provided by this Act.

##### **Biometric measures in the public sector**

###### Article 79

- (1) Biometric measures in the public sector may only be provided for by statute if it is necessarily required for the security of people or property or to protect secret data and business secrets, and this purpose cannot be achieved by milder means.
- (2) Irrespective of the previous paragraph, biometric measures may be provided by statute where they involve compliance with obligations arising from binding international treaties or for identification of individuals crossing state borders.

##### **Biometric measures in the private sector**

###### Article 80

- (1) The private sector may implement biometric measures only if they are necessarily required for the performance of activities, for the security of people or property, or to protect secret data or business secrets. Biometric measures may only be used on employees if they were informed in writing thereof in advance.
- (2) If the implementation of specific biometric measures in the private sector is not regulated by statute, a data controller intending to implement biometric measures shall prior to introducing the measures be obliged to supply the National Supervisory Body with a description of the intended measures and the reasons for the introduction thereof.

(3) The National Supervisory Body shall on receipt of information from the previous paragraph be obliged within two months to decide whether the intended introduction of biometric measures complies with this Act, and in particular with the conditions from the first sentence of the first paragraph of this Article. The deadline may be extended by a maximum of one month if the introduction of such measures would affect more than 20 employees in a person in the private sector, or if the representative trade union at the employer requests to participate in the administrative procedure.

(4) The data controller may implement biometric measures upon receipt of a decision from the previous paragraph whereby the implementation of biometric measures is permitted.

(5) There shall be no appeal against a decision of the National Supervisory Body from the third paragraph of this Article, but an administrative dispute shall be permitted.

### **Biometric measures in connection with public sector employees**

#### Article 81

Irrespective of the provision of Article 79 of this Act, biometric measures may be implemented in the public sector in connection with entry into a building or parts of a building and recording the presence of employees at work, and they shall be implemented with the *mutatis mutandis* application of the second, third and fourth paragraphs of Article 80 of this Act.

## **Chapter 4**

### **Records of entry to and exit from premises**

#### **Records**

#### Article 82

(1) Persons in the public or private sector may, for the purposes of protecting property or the life and bodies of individuals, and order in their premises, require individuals intending to enter or leave such premises to state all or some of the personal data from the second paragraph of this Article and the reason for entry or exit. If required, the personal data may be verified by examining a personal document of the individual.

(2) The records of entry and exit may only contain the following personal data for individuals: personal name, number and type of personal document, address of permanent or temporary residence, employment, and the date of, time of and reason for entry or exit to or from the premises.

(3) Records from the previous paragraph shall be regarded as official records in accordance with the statute regulating the general administrative procedure, if the acquisition of data is required in terms of benefiting a minor or for the implementation of the competences of the police, and intelligence-security activities.

(4) Personal data from the records from the second paragraph of this Article may be stored for a maximum of three years from their recording, and then shall be erased, unless otherwise provided by statute.

## **Chapter 5**

### **Public books and protection of personal data**

#### **Statutory purpose of public books**

##### Article 83

Personal data from public books regulated by statute may only be used in accordance with the purpose for which they were collected or are processed, if the statutory purpose of their collection or processing is defined or definable.

## **Chapter 6**

### **Linking filing systems**

#### **Official records and public books**

##### Article 84

(1) Filing systems from official records and public books may be linked if so provided by statute.

(2) Data controllers or a data controller linking two or more filing systems kept for different purposes shall be obliged to inform the National Supervisory Body in writing thereof in advance.

(3) If at least one filing system to be linked contains sensitive data, or if the linking would result in disclosure of sensitive data, or if implementation of the linking requires the use of the same connecting code, linking shall not be permitted without the prior permission of the National Supervisory Body.

(4) The National Supervisory Body shall permit linking from the previous paragraph on the basis of a written application of the data controller if it determines that the data controller ensures adequate protection of personal data.

(5) There shall be no appeal against decisions from the previous paragraph, but an administrative dispute shall be permitted.

#### **Prohibition of linking**

##### Article 85

Linking filing systems from criminal record and minor offence records to other filing systems, and linking filing systems from criminal records and minor offence records, shall be prohibited.

## **Special provisions**

### Article 86

Data on linked filing systems from official records and public books shall be kept separately in the Register of Filing Systems.

## **Chapter 7**

### **Expert supervision**

#### **Application of the provisions of this Chapter**

### Article 87

Unless otherwise provided by another statute, the provisions of this Chapter shall apply for the processing of personal data in expert supervision provided by the statute<sup>28</sup>.

### **General provisions**

### Article 88

(1) Public sector person performing expert supervision (hereinafter: implementer of expert supervision) may process personal data processed by data controllers over whom by statute he is competent to implement expert supervision.

(2) Expert supervisor shall have the right to consult, extract, transcribe or copy all personal data from the previous paragraph, but during their processing for the purposes of expert supervision and production of a report or assessment he shall be bound to protect their secrecy. In report or assessment upon the conclusion of expert supervision, implementer of expert supervision may note down only those personal data that are essential for achieving the purpose of the expert supervision.

(3) The costs of consultation, extraction, transcription or copying from the previous paragraph shall be borne by the data controller.

#### **Expert supervision and further processing of personal data**

### Article 89

(1) In performing expert supervision, where in accordance with the first paragraph of Article 88 of this Act personal data are processed, implementer of expert supervision may inform in writing the individual to whom the personal data relate, that he is performing expert supervision and inform the individual that he may give his opinion in writing or orally.

(2) The individual from the previous paragraph may supply to the implementer of expert supervision for the purposes of performing expert supervision the personal data of another

---

<sup>28</sup> This means other statutes, not the Personal Data Protection Act.

individual that may know something about the matter in which expert supervision is being performed. If the implementer of expert supervision deems it necessary, he may conduct an interview also with the other individual.

### **Expert supervision and sensitive personal data**

#### Article 90

If in the performance of expert supervision sensitive personal data are processed, the implementer of expert supervision shall make an official annotation or other official record of this in the case file of the data controller.

## **PART VII**

### **PENAL PROVISIONS**

#### **General violations of the provisions of this Act**

#### Article 91

(1) A fine of between SIT 1,000,000 and 3,000,000 shall be imposed for a minor offence on a legal person or sole trader:

1. if he processes personal data without having the statutory grounds or personal consent of the individual to so do (Article 8);
2. if he entrusts an individual task relating to the processing of personal data to another person without concluding a contract in accordance with the second paragraph of Article 11;
3. if he processes sensitive personal data in contravention of Articles 13 or does not protect them in accordance with Article 14;
4. if he automatically processes personal data in contravention of Article 15;
5. if he collects personal data for purposes that are not defined and lawful<sup>29</sup>, or if he continues to process them in contravention of Article 16;
6. if he supplies to a data recipient personal data in contravention of the second paragraph of Article 17 or if he does not destroy personal data in accordance with the third paragraph of Article 17 or does not publish the results of processing in accordance with the fourth paragraph of Article 17;
7. if he does not inform the individual of the processing of personal data in accordance with Article 19;
8. if he uses the same linking code in contravention of Article 20;

---

<sup>29</sup> Verbatim: statutory (in accordance with a statute).

9. if he does not delete, destroy, block or anonymise personal data after the purpose for which they were processed has been achieved in accordance with the second paragraph of Article 21;
  10. if he acts in contravention of Article 22;
  11. if he fails to ensure that the filing system catalogue contains data provided by statute (Article 26);
  12. if he fails to supply data for the needs of the Register of Filing Systems (Article 27);
  13. if he acts in contravention of the first or second paragraphs of Article 30 or the second, third or fifth paragraphs of Article 31;
  14. if he acts in contravention of Article 32 or the second or fifth paragraphs of Article 33;
  15. if he acts in contravention of the first paragraph of Article 63 or in contravention of Article 70 transfers personal data to a third country;
- (2) A fine of between SIT 200,000 and 500,000 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person or the sole trader.
  - (3) A fine of between SIT 200,000 and 500,000 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.
  - (4) A fine of between SIT 50,000 and 200,000 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

### **Violation of the provisions on contractual processing**

#### Article 92

- (1) A fine of between SIT 1,000,000 and 3,000,000 shall be imposed for a minor offence on a legal person or sole trader, if he oversteps the authorisation contained in the contract from the second paragraph of Article 11 or does not return personal data in accordance with the third paragraph of Article 11.
- (2) A fine of between SIT 200,000 and 500,000 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person or the sole trader.
- (3) A fine of between SIT 200,000 and 500,000 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.
- (4) A fine of between SIT 50,000 and 200,000 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

### **Violation of the provisions on security of personal data**

#### Article 93

- (1) A fine of between SIT 1,000,000 and 3,000,000 shall be imposed for a minor offence on a legal person or sole trader, if he processes personal data in accordance with this Act and fails to ensure security of personal data (Articles 24 and 25).
- (2) A fine of between SIT 200,000 and 300,000 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person or the sole trader.
- (3) A fine of between SIT 200,000 and 300,000 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.
- (4) A fine of between SIT 50,000 and 200,000 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

### **Violation of the provisions on direct marketing**

#### Article 94

- (1) A fine of between SIT 500,000 and 1,000,000 shall be imposed for a minor offence on a legal person or sole trader, if in accordance with this Act he processes personal data for the purposes of direct marketing and does not act in accordance with Articles 72 or 73.
- (2) A fine of between SIT 200,000 and 300,000 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person or the sole trader.
- (3) A fine of between SIT 50,000 and 200,000 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

### **Violation of general provisions on video surveillance**

#### Article 95

- (1) A fine of between SIT 1,000,000 and 3,000,000 shall be imposed for a minor offence on a legal person or sole trader:
  1. if he does not publish a notice in the manner set out in the second paragraph of Article 74;
  2. if the notice does not contain the information from the third paragraph of Article 74;
  3. if he does not protect the video surveillance system used to perform video surveillance in contravention of the fifth paragraph of Article 74.
- (2) A fine of between SIT 200,000 and 300,000 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person or the sole trader.

(3) A fine of between SIT 200,000 and 300,000 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine of between SIT 50,000 and 200,000 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

**Violation of the provisions on video surveillance regarding access to official office premises and business premises**

Article 96

(1) A fine of between SIT 1,000,000 and 3,000,000 shall be imposed for a minor offence on a legal person or sole trader:

1. if he implements video surveillance without an explained written decision or without other legal grounds from the first paragraph of Article 75;

2. if he implements video surveillance so as to show recordings of the interior of residential buildings that do not affect access to his premises or recordings of entrances to apartments (second paragraph of Article 75);

3. if he does not inform employees in writing (third paragraph of Article 75);

4. if he stores personal data in contravention of the fifth paragraph of Article 75.

(2) A fine of between SIT 200,000 and 300,000 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person or the sole trader.

(3) A fine of between SIT 200,000 and 300,000 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine of between SIT 50,000 and 200,000 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

**Violation of the provisions on video surveillance in apartment buildings**

Article 97

(1) A fine of between SIT 500,000 and 2,000,000 shall be imposed for a minor offence on a legal person or sole trader, who implements video surveillance in contravention of Article 76.

(2) A fine of between SIT 100,000 and 300,000 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person or the sole trader.

(3) A fine of between SIT 200,000 and 300,000 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine of between SIT 50,000 and 100,000 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

#### **Violation of the provisions on video surveillance in work areas**

##### Article 98

(1) A fine of between SIT 1,000,000 and 3,000,000 shall be imposed for a minor offence on a legal person or sole trader, who implements video surveillance in work areas in contravention of Article 77.

(2) A fine of between SIT 300,000 and 500,000 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person or the sole trader.

(3) A fine of between SIT 300,000 and 500,000 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine of between SIT 200,000 and 300,000 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

#### **Violation of the provisions on biometrics in the public sector**

##### Article 99

(1) A fine of between SIT 1,000,000 and 3,000,000 shall be imposed for a minor offence on a legal person in the public sector who implements biometric measures in contravention of Article 79.

(2) A fine of between SIT 300,000 and 500,000 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person in the public sector.

(3) A fine of between SIT 300,000 and 500,000 shall be imposed for a minor offence from the first paragraph of this Article on the responsible person of the state body or body of self-governing local community who commits the act from the first paragraph of this Article.

#### **Violation of the provisions on biometrics in the private sector**

##### Article 100

(1) A fine of between SIT 1,000,000 and 3,000,000 shall be imposed for a minor offence on a legal person or sole trader, who implements biometric measures in contravention of Article 80.

(2) A fine of between SIT 300,000 and 500,000 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person or the sole trader.

### **Violation of the provisions on records of entry and exit**

#### Article 101

(1) A fine of between SIT 500,000 and 1,000,000 shall be imposed for a minor offence on a legal person or sole trader:

1. who uses entry and exit records as official records in contravention of the third paragraph of Article 82;

2. who acts in contravention of the fourth paragraph of Article 82.

(2) A fine of between SIT 50,000 and 200,000 shall be imposed for a minor offence on the responsible person of the legal person or the sole trader who commits a minor offence from the previous paragraph.

(3) A fine of between SIT 50,000 and 200,000 shall be imposed for a minor offence on the responsible person of the state body or body of self-governing local community who commits a minor offence from the first paragraph of this Article.

(4) A fine of between SIT 50,000 and 100,000 shall be imposed for a minor offence on the individual who commits a minor offence from the first paragraph of this Article.

### **Violation of the provisions on linking filing systems**

#### Article 102

(1) A fine of between SIT 200,000 and 500,000 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community, who links filing systems in contravention of the third paragraph of Article 84.

(2) A fine of between SIT 200,000 and 500,000 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community, who links filing systems from criminal record and minor offence records with other filing systems, or links filing systems from criminal records with filing systems from records on minor offences (Article 85).

### **Violation of the provisions on expert supervision**

#### Article 103

(1) A fine of between SIT 1,000,000 and 3,000,000 shall be imposed for a minor offence on a legal person:

1. if he performs expert supervision in contravention of the second paragraph of Article 88;

2. if he does not make an official annotation or other official record in contravention of Article 90 of this Act.

(2) A fine of between SIT 200,000 and 300,000 shall be imposed for a minor offence from the previous paragraph on the responsible person of the legal person.

(3) A fine of between SIT 300,000 and 500,000 shall be imposed for a minor offence on the responsible person of a state body or body of self-governing local community who commits the act from the first paragraph of this Article.

(4) A fine of between SIT 50,000 and 200,000 shall be imposed for a minor offence on an individual who commits the act from the first paragraph of this Article.

## **PART VIII**

### **TRANSITIONAL AND FINAL PROVISIONS**

#### **Competences of the Commissioner for Access to Information of a Public Character regarding protection of personal data**

##### Article 104

(1) Until the entry into force of the statute governing this issue, the Commissioner for Access to Information of a Public Character may initiate an administrative dispute against a decision or resolution of the National Supervisory Body, if he determines that this has violated access to information of a public nature.

(2) The administrative dispute procedure from the previous paragraph shall be urgent and a priority.

(3) The Commissioner for Access to Information of a Public Character shall be bound to deliver to the National Supervisory Body a decision or resolution in which he has taken a position regarding the issue of protection of personal data.

#### **Deadline for issuing implementing regulations**

##### Article 105

(1) The rules from the third paragraph of Article 28 and Article 69 of this Act shall be issued within two months of the entry into force of this Act.

(2) The regulation from the second paragraph of Article 52 of this Act shall be issued by 1 January 2006.

#### **Transitional arrangements**

##### Article 106

(1) Public funds may on the basis of personal consent from individuals process and collect personal data relating to them if such data are necessary and appropriate for the implementation of their tasks and competences, irrespective of the provisions of statutes regulating their tasks and competences and of the provisions of this Act until the entry into force of a special statute regulating this issue.

(2) Data controllers may supply to the public and publish the personal name, title or function, official telephone number and official electronic mail address of the head and those employees whose work is important for operations with clients or users of services, until the entry into force of a special statute regulating this issue.

### **The term data controller**

#### Article 107

The terms "filing system controller", "controller of data", "databases controller" or "database controller" which are provided in statutes shall be deemed to mean the term "data controller" under this Act.

### **Start of operation of the National Supervisory Body for Personal Data Protection**

#### Article 108

(1) The National Supervisory Body for Personal Data Protection shall begin to operate on 1 January 2006.

(2) Until the National Supervisory Body for Personal Data Protection starts to operate, its competences and tasks under this Act shall be performed by the Inspectorate for Personal Data Protection of the Republic of Slovenia as a body within the Ministry of Justice and by Inspectors appointed pursuant to the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01- correction, 52/02-ZDU-1 and 73/04 – ZUP-C).

### **Appointment of the Chief National Supervisor**

#### Article 109

(1) The procedure for appointment of the Chief National Supervisor shall start no later than on 1 June 2005.

(2) On the day of the appointment of the Chief National Supervisor, the term of office of the Chief Inspector for Personal Data Protection shall cease.

(3) If the Chief National Supervisor is appointed prior to the start of work of the National Supervisory Body for Personal Data Protection, the Chief National Supervisor shall be the head of the Inspectorate for Personal Data Protection of the Republic of Slovenia as a body within the Ministry of Justice up until the start of work by the National Supervisory Body for Personal Data Protection.

(4) If the Chief National Supervisor is not appointed by the time the National Supervisory Body for Personal Data Protection begins working, his function shall be performed by the Chief Inspector for Personal Data Protection as Acting Chief National Supervisor until the appointment is made.

### **Take-over of employees and archives**

#### Article 110

(1) The National Supervisory Body for Personal Data Protection shall take over Inspectors and other employees who on the day the National Supervisory Body for Personal Data Protection begins operating are performing work at the Inspectorate for Personal Data Protection of the Republic of Slovenia.

(2) Unfinished matters, archives and records maintained by the Inspectorate for Personal Data Protection of the Republic of Slovenia shall be transferred to the National Supervisory Body for Personal Data Protection.

### **Application of individual provisions of this Act**

#### Article 111

(1) The provisions of the second paragraph of Article 48 and subparagraphs 3 and 4 of the first paragraph of Article 49 of this Act shall start to apply on the day the National Supervisory Body for Personal Data Protection begins operating.

(2) Until the establishing of the website of the National Supervisory Body for Personal Data Protection, the information which the National Supervisory Body shall publish under this Act on its website shall be published on the website of the Ministry of Justice.

### **Completion of current proceedings**

#### Article 112

If a decision or ruling of an Inspector has been issued prior to the entry into force of this Act, the procedure shall be completed under the provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01- correction, 52/02-ZDU-1 and 73/04 – ZUP-C).

### **Transfer of management of the Register of Filing Systems**

#### Article 113

(1) The Joint Catalogue of Personal Data managed under the provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01 – correction, 52/02 – ZDU-1 and 73/04 – ZUP-C), shall on the date of entry into force of this Act be renamed the Register of Filing Systems.

(2) Until 1 January 2006 the Register from the previous paragraph shall be managed and maintained by the Ministry of Justice, and on that date it shall be handed over to the National Supervisory Body for Personal Data Protection.

### **Supplement to data in the Register of Filing Systems**

#### Article 114

Data controllers who have supplied personal data under the provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01 – correction, 52/02 – ZDU-1 and 73/04 – ZUP-C) to the Joint Catalogue of Personal Data must supply all data from Article 27 of this Act to the competent body from Article 113 of this Act within one year of the entry into force of the implementing regulation from the third paragraph of Article 28 of this Act.

### **Cessation of validity**

#### Article 115

(1) On the day this Act enters into force, the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01- correction, 52/02-ZDU-1 and 73/04 – ZUP-C) shall cease to have effect.

(2) On the day the National Supervisory Body for Personal Data Protection begins operating, the second subparagraph of the first paragraph and the third paragraph of Article 13 of the Regulation on Bodies within Ministries (Official Gazette of the Republic of Slovenia, No. 58/03) shall cease to have effect.

(3) On the day this Act enters into force, the provisions of the first paragraph of Article 110 and the second paragraph of Article 111 of the Electronic Communications Act (Official Gazette of the Republic of Slovenia, No. 43/04) shall cease to have effect in that part laying down the collection, processing and publication of the EMŠO – the standardised personal registration number.

### **Amendment of other statute**

#### Article 116

In the Act Ratifying the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Official Gazette of the Republic of Slovenia, No. 11/94 – International Treaties, No. 3/94) in Article 3 the wording "science and technology" shall be replaced by wording "justice".

### **Entry into Force**

#### Article 117

This Act shall enter into force on 1 January 2005.

No. 210-01/89-3/25

Ljubljana, 15 July 2004  
EPA 1228-III

President  
of the National Assembly  
of the Republic of Slovenia  
**Feri Horvat (signed)**

---

**Disclaimer:** The English language translation of the text of the Personal Data Protection Act (of the Republic of Slovenia) above is provided just for information only and confers no rights nor imposes any obligations on anyone. Only the official publication of the Personal Data Protection Act in Slovene language, as published and promulgated in the Official Gazette of the Republic of Slovenia, is authentic. The status of the translated text of the Personal Data Protection Act is as of 17 October 2005 and the status of statutes and other information in footnotes and in Appendixes is also as of 17 October 2005. The explanatory footnotes and appendices have also been inserted just for information only, and previous text of this Disclaimer also applies to them. While the Government Translation Service prepared the original translation, Ministry of Justice of the Republic of Slovenia performed the substantially corrected translation, terminology decisions and annotations. This translation may not be published in any way, without the prior permission of the Ministry of Justice of the Republic of Slovenia, but may be used for information purposes only. Further editorial revisions of this translation are possible.

---

## Appendix 1

### **The Constitution of the Republic of Slovenia<sup>30</sup>**

#### Article 38

##### **(Protection of Personal Data)**

The protection of personal data shall be guaranteed. The use of personal data contrary to the purpose for which it was collected is prohibited.

The collection, processing, purpose of use, supervision and protection of the secrecy of personal data shall be provided by statute.

Everyone has the right of access to the collected personal data that relate to him and the right to judicial protection in the event of abuse of such data.

---

## Appendix 2

### **The Criminal Code of the Republic of Slovenia<sup>31</sup>**

#### **Statutory Rehabilitation and Deletion of Conviction**

##### Article 103

(1) By means of statutory rehabilitation, the conviction shall be deleted from the criminal record, the legal consequences of the conviction shall cease to apply and the convicted person shall be deemed never to have been convicted.

(2) The conviction shall be understood to mean final decision as well as any modification of such a decision by means of amnesty or pardon.

(3) The conviction shall be deleted from the criminal record within the prescribed period of time from the day the punishment was enforced, barred by the statute or remitted, unless in such a period the convicted person commits another criminal offence.

(4) Time periods under the preceding paragraph shall be as follows:

- 1) one year from the finality of the court decision in which by a conviction a court admonition was administered to the perpetrator or his punishment was remitted;
- 2) one year from the expiry of the term of suspension if the case of a conviction by probation;

---

<sup>30</sup> Official Gazette of the Republic of Slovenia, Nos. 33/91-I, 42/97, 66/2000, 24/2003 and 69/2004. Constitution of the Republic of Slovenia is in Slovene language: "Ustava Republike Slovenije".

<sup>31</sup> Official Gazette of the Republic of Slovenia, Nos. 63/94, 70/94 – correction, 23/99, 40/2004 and 95/2004 - officially consolidated text. Criminal Code is in Slovene language: "Kazenski zakonik".

- 3) three years, for a conviction by a fine, accessory punishment, a punishment by imprisonment of up to one year or to juvenile imprisonment;
  - 4) five years, for a conviction to punishment by imprisonment between one and up to three years;
  - 5) eight years, for a conviction to a punishment by imprisonment of between three and up to five years;
  - 6) ten years, for a conviction to a punishment by imprisonment of between five and up to ten years;
  - 7) fifteen years, for conviction to a punishment by imprisonment of between ten and up to fifteen years.
- (5) A conviction to punishment by imprisonment above fifteen years shall not be deleted from the criminal record.
- (6) A conviction may not be deleted as long as security measures apply [to the perpetrator].

### **Court Rehabilitation**

#### Article 104

Upon a request from the convicted person, the court may rule that the conviction be deleted from the criminal record and that the convicted person be deemed never to have been convicted, provided that half of the statutorily prescribed period has elapsed by expiry of which the conviction is removed, and with the further proviso that during this period the convicted person has not committed another criminal offence. In decision-making whether to delete the conviction the court shall consider the convicted person's behaviour after he has served his punishment and the nature of the criminal offence [he committed], as well as other circumstances relevant to the deletion of the conviction.

### **Release of Data from the Criminal Record**

#### Article 105

- (1) The criminal record shall contain the following: personal data on perpetrators of criminal offences; information on the imposed punishments, security measures, convictions by probation, court admonitions and the remitted punishments referring to the perpetrators of which a record is being kept; as well as the legal consequences incident to them; later alterations of data on convictions that were entered in the criminal record; as well as data on the enforced punishments and on the annulment of the entry of unjustified conviction.
- (2) A special record shall be kept with respect to educational measures. It shall contain personal data on a juvenile, data on the educational measures imposed and enforced, as well as all other data relating to the enforcement of educational measures.
- (3) Data from the criminal record may be released only with respect to convictions that have not been deleted to the court, the state prosecutor's office and bodies of the law enforcement dealing with criminal proceedings against a previously convicted person, bodies responsible for the enforcement of penal sanctions and bodies involved in the procedures for granting an amnesty, pardon or for deleting a conviction.

(4) Data on a conviction which was not deleted may be released to the state bodies, legal persons and private employers upon a reasoned request only if the legal consequences of the conviction or of the security measures are still in effect or if such persons show a legitimate and legally-grounded interest.

(5) Upon his request, an individual may be provided with data on whether he was convicted or not only when he needs them for the assertion of his rights.

(6) Data with respect to convictions that have not been deleted and were imposed on citizens of the Republic of Slovenia by foreign courts may only be released to the bodies from paragraph 3 of this Article as well as to the bodies from Article 86 of this Code.

(7) Provisions on statutory rehabilitation and deletion of conviction (Article 103) and on court rehabilitation (Article 104) are to be applied *mutatis mutandis* also in case of a judgment that was imposed on the Slovenian citizen by a foreign court.

### **Abuse of Personal Data**

#### Article 154

(1) Whoever contrary to the statute uses personal data, which may be kept only on the basis of the statute or on the basis of the personal consent of the individual to whom the personal data relate,

shall be punished by a fine or by imprisonment of up to one year.

(2) Whoever breaks into filing system kept by computer in order to acquire personal data for himself or a third person,

shall be punished the same [in accordance with the preceding paragraph of the present Article].

(3) If any offence from the preceding two paragraphs is committed by an official person through the abuse of official position or rights of office,

[he] shall be punished by imprisonment of up to two years.

---

## Appendix 3

### **The Obligations Code of the Republic of Slovenia<sup>32</sup>**

#### **Request to Cease Infringement of Personality Rights**

##### Article 134

(1) All persons shall have the right to request the court or any other relevant authority to order that action that infringes the inviolability of the human person, personal and family life or any other personality right be ceased, that such action be prevented or that the consequences of such action be eliminated.

(2) The court or other relevant authority may order that the violator cease such action, with failure to do so resulting in the mandatory payment of a monetary sum to the person affected, levied in total or per time unit.

#### **Reimbursement of Material Damage in Case of Defamation or Calumny**

##### Article 177

(1) Any person that defames another or asserts or disseminates untrue statements on the past, knowledge or capability of another, even though the former knows or should have known that they were untrue, and thereby inflicts material damage on the latter must reimburse such damage.

(2) However any person that reports anything untrue about another without knowing that such was untrue shall not be liable for the damage inflicted if there was a serious interest in so doing for the former or the person to whom the report was made.

#### **Publication of Judgement or Correction**

##### Article 178

In a case of the infringement of a personality right the court may order the publication of the judgement or a correction at the injurer's expense or order that the injurer must retract the statement by which the infringement was committed or do anything else through which it is possible to achieve the purpose achieved via compensation.

---

<sup>32</sup> Official Gazette of the Republic of Slovenia, Nos. 83/2001 and 32/2004 - authentic interpretation of Article 195. Obligations Code is in Slovene language: "Obligacijski zakonik".

## **Monetary Compensation**

### Article 179

(1) Just monetary compensation independent of the reimbursement of material damage shall pertain to the injured party for physical distress suffered, for mental distress suffered owing to a reduction in life activities, disfigurement, the defamation of reputation or honour, the truncation of freedom or a personality right, or the death of a close person, and for fear, if the circumstances of the case, particularly the level and duration of distress and fear, so justify, even if there was no material damage.

(2) The amount of compensation for non-material damage shall depend on the importance of the good affected and the purpose of the compensation, and may not support tendencies that are not compatible with the nature and purpose thereof.