PERSONAL DATA PROTECTION ACT

- 1. Introduction 1
- 2. Personal data protection 3
- 3. Security of personal data 4
- 4. Data catalogues and database catalogues 5
- 5. The rights of an individual 6
- 6. Protection of the rights of an individual 8
- 7. Restrictions on the rights of an individual 8
- 8. Conveyance of personal data outside the country 9
- 9. Inspection and supervision 9
- 10. Monitoring the enforcement of the act 11
- 11. Penal provisions 11
- 12. Transitional and final provisions 12

(Zakon o varstvu osebnih podatkov, ZVOP, Ur.l. RS No. 59/99)

1. Introduction

Article 1

Personal data protection shall prevent any illegal and unwarranted violations of personal privacy in the course of data-processing, the securing of personal databases and the use thereof.

Article 2

The meaning of the terms used in this Act shall be as follows:

1. Personal data — data which indicates the properties, situation or relationship of an individual, regardless of the form in which it is given;

2. Individual — a specific or identifiable natural person to whom this data refers; a natural person shall be identifiable when identifiable in a manner which does not incur large costs or require a large amount of time;

3. Data-processing - the collection, storage or merging of data in databases; the change, use or imparting, including transfer, search for, blocking and deletion of data; processing can be either manual or by means of information technology;

4. Database — any data string which contains at least one personal data item, regardless of whether it is kept in a centralised form or organised and structured pursuant to the criteria enabling the use or merging of data, and regardless of whether the processing is performed through information technology means;

5. Database administrator — a natural person or legal entity authorised by law or the written consent of the individual to whom data refers, to set up, maintain and supervise a database;

6. Data user — a natural person or legal entity authorised to use personal data by law, written request or the consent of the individual to whom data refers;

7. Written consent of an individual — the signed written consent of an individual to have certain data on him processed for specific purposes, which may be given in the form of a document, a contractual provision, the provisions of an order, the supplement to an application, or any other form, in keeping with a special act.

8. Blocking — any change to the form of personal data after which such data can no longer be associated with an individual or could only be associated with an individual after investing a disproportionate amount of effort, funds or time.

Article 3

Personal data may only be processed if data-processing is determined by law or if the database administrator has acquired the written consent of the individual.

State bodies, local community bodies and holders of public authorisations may process only such personal data for which they have been authorised by law.

Database administrators authorised by law to collect data may collect personal data on racial or other origins, political, religious or other beliefs, trade union membership or sexual behaviour solely on the basis of the written consent of the individual. An act may be used to determine other types of personal data which may be collected by database administrators on the basis of the written consent of the individual.

The provision of the first paragraph of this Article notwithstanding, legal entities or natural persons performing a public service or activity under the Commercial Companies Act shall process personal data on persons who are in a contractual relationship with them if such data is required in order to fulfil contractual obligations or to exercise rights arising from a contractual relationship.

When personal data is processed on the basis of the written consent of an individual, that individual must first be informed in writing of the purpose of the data-processing and, in particular, of the purpose of its use and the duration of its storage.

Article 4

The processing of personal data on racial or other origins, political, religious and other beliefs, trade union membership, sexual behaviour, criminal convictions and medical data must be specially labelled and protected.

Personal data from the preceding paragraph may be transferred by means of telecommunications networks only if these are specially protected by encryption methods and by an electronic signature which guarantees its illegibility during transfer.

Article 5

The provisions of this Act shall not be used for the following:

1. personal data in a database for which the individual has given written consent to the effect that it may be kept in the database and which, by its nature or purpose, may be accessed by anyone;

2. personal data collected by parties, societies and other similar organisations on their members, if they so agree;

3. personal data which is part of the name or title of a company, branch office or other organisation or institution;

4. personal data contained in books, publications and other material kept by museums, libraries, archives and similar public institutions, because they are public and accessible to all.

Article 6

Any individual, regardless of their nationality and place of residence, shall be guaranteed personal data protection on the territory of the Republic of Slovenia.

2. Personal data protection ➦

Article 7

A database administrator may entrust tasks associated with personal data-processing to another natural person or legal entity registered for the performance of such an activity.

A person from the preceding paragraph may only engage in personal data-processing within the scope of the authorisation accorded by a client, and may not process or use personal data in any other way. Mutual rights and obligations shall be regulated in a contract, which must be concluded in writing and must contain the conditions and measures for ensuring the protection and security of personal data.

Article 8

Personal data shall be obtained directly from the individual.

In individual instances it may be determined by law that personal data may also be collected from other persons or obtained from existing databases, whereby the person, database, type of data and manner of data collection must be specified. When obtaining data from existing databases, the purposes for which it was collected must be taken into account.

Personal data on national, racial or other origins, political, religious and other beliefs, education, medical condition (except for contagious diseases), and sexual behaviour may be obtained from other persons or acquired and linked from existing personal databases solely on the basis of the written consent of the individual to whom it refers, except when the user intends to use personal data for statistical or scientific research purposes in a form which renders it impossible to identify the individuals to whom it refers, whereby the database and the type of personal data and the manner of collection must be specified.

The use of the same connecting code when acquiring personal data from databases covering the areas of public security, national security, national defence, justice and healthcare shall not be permitted.

Article 9

Personal data may only be processed for the purposes laid down by law or with the written consent of the individual, and may not be used in a manner which is incompatible with those purposes.

Article 10

Personal data may be stored and used only for as long as it is necessary to achieve the purpose for which it was processed.

Unless otherwise stipulated in acts on individual types of personal data, personal data shall either be deleted from a personal database or blocked once the purpose from the preceding paragraph has been achieved.

Article 11

Unless otherwise stipulated, a personal database administrator must impart personal data to users against payment for the service of imparting the data.

The administrator may impart personal data to a user who is not a personal data user under this Act only if this user intends to use such personal data for statistical or scientific research purposes in a form which renders identification of the individual impossible.

The administrator of the central population register may, pursuant to a written request, supply the users from the preceding paragraph with the name, surname, profession and address of an individual who has been informed of such a possibility and who did not forbid the imparting of data, if such data is required to develop statistical or other research patterns or to obtain the written consent of the individual.

The administrator of the central population register or the administrator of records of permanent or temporary residents must, in the manner determined for issuing a certificate, supply an individual or legal entity or other organisation with the name, surname and address of the person against whom they are exercising or protecting their rights from state bodies, local community bodies or holders of public authorisations.

For each separate imparting of personal data, the database administrator must ensure that it is possible subsequently to establish which personal data was imparted, to whom and on what grounds, during the period when legal protection of the rights of an individual can be exercised due to the impermissibility of imparting personal data.

A data user and the administrator from the third paragraph of this Article and the individual, legal entity or other organisation from the fourth paragraph of this Article must treat the supplied personal data in keeping with the provisions of this Act.

Article 12

A data administrator may impart personal data on a deceased person to users if the user can prove his legal interest in using personal data on the deceased person, and if the deceased person, when still alive, did not specifically forbid the imparting of his personal data and if his immediate family members do not object.

3. Security of personal data ➦

Article 13

The security of personal data shall include organisational and appropriate logistic and technical procedures and measures for securing personal data, preventing the accidental or intentional unauthorised destruction of data, or changes to or loss of data, as well as any unauthorised data-processing, by:

1. protecting premises, hardware (including input-output units) and system software;

2. protecting the applications software for personal data-processing;

3. preventing unauthorised access to personal data during transfer, including during transfer by means of telecommunications networks;

4. making it possible to establish subsequently when individual personal data items have been used or entered into a database and by whom, for the period when the legal protection of the rights of an individual can exercised against any unauthorised imparting of personal data.

In instances of data-processing accessible by telecommunications networks, the hardware, system software and applications software must ensure that the processing of the data contained in databases is conducted within the scope of the authorisations of the personal data user.

Article 14

The procedures and measures from the preceding paragraph shall be laid down in internal regulations of data administrators, processors and users, who shall also ensure the implementation thereof.

4. Data catalogues and database catalogues ➦

Article 15

The database administrator shall ensure for each database a data catalogue, which shall contain the following:

1. the name of the personal database;

2. the identity of the personal database administrator and his head office;

3. the legal grounds for setting up the database;

4. the categories of individuals;

5. the types of personal data stored in the database;

6. the legal grounds for the collection of personal data;

7. the method of personal data collection;

8. the purpose and legal grounds of the collection, processing, storage and use of personal data;

9. the time-limit for the storage and use of personal data;

10. the restrictions on the rights of individuals regarding the data stored in the database, and the legal grounds for these restrictions;

11. the users of personal data stored in the database;

12. whether personal data will be conveyed outside the country, where, to whom, and the legal grounds for this;

13. a description of security measures.

Article 16

The personal data administrator shall convey the information from the first, second, fourth and fifth points of the preceding paragraph to the ministry responsible for personal data protection, which in keeping with the law shall keep the catalogue of databases (joint data catalogue), 15 days before setting up the database or before entering a new type of personal data.

The personal database administrator shall also forward to the ministry from the preceding paragraph the information on any alterations to the data from the preceding Article within seven days of the day of such alteration.

The ministry from the first paragraph of this Article shall publish the database catalogue in the manner and at intervals set by the regulation on the methods of keeping the catalogue.

5. The rights of an individual ➦

Article 17

The ministry which keeps and maintains the database catalogue must permit any person, upon written or oral request, to access the database catalogue and copy the data.

The ministry must, as a rule, permit and enable access on the same day and no later than within seven days, otherwise the request shall be considered to have been denied.

Article 18

The database administrator must, upon the request of an individual:

1. enable that individual to access the personal database catalogue, access personal data contained therein which refers to him, and to copy such data;

2. provide that individual with a copy of the personal data contained in the database which refers to him;

3. supply that individual with a list of all those who were, in keeping with the fifth paragraph of Article 11 of this Act, provided within a specified period with personal data from the database which refers to him;

4. enable the individual to access sources for entries on him in the database and on the processing method.

The request from the preceding paragraph shall be filed, in writing or orally for the record, with the database administrator.

The personal database administrator must enable an individual to access and copy personal data under point 1 of the first paragraph of this Article no later than 15 days from the day the request was received, or shall, within the same period, inform the individual in writing of the reasons for denying access and copying.

The personal database manager must supply the copy from the second point of this Article and the list from the third point of the first paragraph of this Article to the individual within 30 days of receiving the request, or shall inform the individual within the same period of the reasons for not supplying the copy or the list.

If the administrator does not act under the third and fourth paragraphs, it shall be considered that the request has been denied.

A copy from the second point of the first paragraph of this Article may not replace a document or certificate under the regulations on administrative or other procedures, which shall also be stated on the copy.

Costs connected with the request and with copying shall be borne by the database administrator.

Article 19

The personal database administrator must, upon the request of an individual:

1. supplement or correct personal data established to be incomplete, inaccurate or out of date;

2. delete any personal data which the individual proves has been collected in violation of the provisions of this Act.

The request from the preceding paragraph shall be made, in writing or orally for the record, to the personal database administrator.

Unless otherwise stipulated by law, should the database administrator establish that personal data is incomplete, inaccurate or out of date, he shall supplement or correct it and shall notify the individual.

The database administrator must supplement, correct or delete data under the first paragraph within 15 days of receiving the request or, within the same period, inform the person who submitted the request of the reasons why the request will not be granted.

The database administrator must immediately inform the data users to whom he imparted data of the supplementation, correction or deletion of personal data.

If the database administrator does not act under the fourth paragraph of this Article, it shall be considered that the request has been denied.

The costs of supplementing, correcting or deleting data, and costs connected with notification, shall be borne by the database manager.

The supplementation, correction or deletion of data shall not exonerate the database manager from possible criminal and material responsibility.

6. Protection of the rights of an individual ➦

Article 20

An individual who considers that his rights under this Act have been violated may file a suit requesting court protection for the entire duration of the violation.

If the violation from the preceding paragraph has ended, the individual may file a suit to establish that the violation did exist.

Unless otherwise stipulated by this Act, the suit shall be ruled on by an administrative court under the provisions of the act governing administrative dispute procedures.

The procedure concerning the suit shall be considered urgent.

Article 21

In the suit in connection with the violation of rights from Article 19 of this Act, the individual may request that, pending the final decision on his request, the court order the database administrator to forbid any use of the data in question.

The public shall be excluded from the procedure to rule on the suit.

Article 22

An individual who, by virtue of the use of personal data which refers to him and which was collected in a manner or for a purpose contrary to the provisions of this Act, has suffered damage may, in accordance with this Act, request indemnity from the party which caused the damage.

7. Restrictions on the rights of an individual ➦

Article 23

The rights of the individual in connection with the protection of personal data may be restricted only exceptionally, in instances provided for by law, for the needs of national security, defence, public safety, the prevention, detection and prosecution of criminal acts or violations of ethical norms in certain professions, fiscal, budgetary and tax affairs, the monitoring of public safety, and the protection of the subject of the data or the rights and freedoms of others to an extent necessary in order to achieve the purpose for which the restriction has been imposed, except when connected to national, racial or other origins,

political, religious and other beliefs, education, medical condition (except contagious diseases), and sexual behaviour.

The preceding paragraph notwithstanding, the right to view the catalogue of databases and to request court protection may not be restricted.

8. Conveyance of personal data outside the country ➦

Article 24

The database administrator may take personal data out of the country and place it at the disposal of foreign users if the country to which the data is being taken has a system of personal data protection which covers foreign citizens as well. A certificate to that effect shall be issued by the ministry responsible for foreign affairs.

Provided the condition under the preceding paragraph has been met, the imparting of personal data to foreign users shall be permitted if it involves personal data imparted on the basis of international treaties, conventions and agreements, and agreements on scientific, business, technical, cultural and similar cooperation.

The first and second paragraphs notwithstanding, a database administrator shall be allowed to convey personal data out of the country and place it at the disposal of foreign users if the individual to whom the data refers gives written consent to that effect and has been informed of the consequences.

The conveyance of personal data outside the country shall be recorded in accordance with the provisions of Article 15 of this Act.

Article 25

The provisions of the preceding Article notwithstanding, the conveyance of personal data outside the country and its placing at the disposal of foreign users shall not be allowed if so stipulated by law.

9. Inspection and supervision ➦

Article 26

The inspection and supervision of the implementation of the provisions of this Act shall be conducted by the ministry responsible for personal data protection.

As part of the inspection, the ministry shall:

- supervise the legality of data-processing;

- supervise the application and suitability of the procedures and measures for personal data protection as laid down by the internal regulations of natural persons and legal entities from Article 14 of this Act;

- supervise the implementation of the provisions of this Act relating to data catalogues,

catalogues of databases, and the recording of the imparting of data to individual users;

- supervise the implementation of the provisions of this Act relating to the conveyance of data out of the country and its placing at the disposal of foreign users.

Article 27

In carrying out inspection and supervision, the inspector shall be entitled to:

- inspect documentation relating to data-processing and the conveyance of data outside the country and its placing at the disposal of foreign users;

- inspect the contents of databases, and of personal data and database catalogues;

- inspect documentation and acts governing the security of personal data;

- inspect premises in which personal data is processed, as well as computer and other equipment and technical documentation;

- check personal data security measures and procedures, and the implementation thereof.

If in the course of activities from the preceding paragraph an inspector establishes that illegalities in connection with personal data protection have been committed, he shall inform the affected parties of his findings, either directly or through the public media.

An inspector must keep any information he learns of in the course of inspection as an official secret.

Article 28

An inspector shall have the right and duty:

1. to decree that the irregularities he has established be removed by a deadline set by him;

2. to forbid data-processing by natural persons and legal entities from Article 14 of this Act who have not ensured or who fail to implement measures and procedures to protect personal data, or who are processing data illegally;

3. ban the conveyance of data outside the country and its placing at the disposal of foreign users if the data is taken out of the country or imparted in violation of the provisions of this Act.

A complaint against a decision from the preceding paragraph may be lodged within five days of its delivery.

A complaint against decisions under the second and third points of the first paragraph shall not delay their implementation. The decision on such complaint must be made within seven days. The decision on the complaint shall be made by the government.

An inspector who, in the course of an inspection, establishes that a violation has been committed must, in the event of a suspected criminal offence, submit a report or propose that a procedure on the offence be instigated in cases of a suspected offence under this

Act.

10. Monitoring the enforcement of the act

Article 29

The state of affairs in the area of personal data protection and the implementation of the provisions of this Act shall be monitored by the competent working body of the National Assembly.

11. Penal provisions

Article 30

A database administrator, legal entity or individual shall be fined between SIT 500,000 and 1,000,000 for committing an offence in the course of the independent performance of an activity if they:

1. process personal data without being authorised by law or without the written consent of the individual (Article 3);

2. entrust to another person individual tasks in connection with the processing of personal data without concluding an agreement to that effect in accordance with the second paragraph of Article 7;

3. collect personal data from other persons or obtain it from existing databases in violation of the law (Article 8);

4. process personal data for purposes other than those stipulated by law or in the written consent of the individual, or use personal data in a manner incompatible with these purposes (Article 10);

5. fail to delete or block personal data after the purpose for which it was processed and stored has been achieved (Article 10);

6. act in violation of the first, third, fourth or fifth paragraphs of Article 11;

7. fail to ensure that a data catalogue contains the data stipulated by law (Article 15);

8. fail to supply information for the needs of a database catalogue (Article 16);

9. act in violation of the first, third or fourth paragraphs of Article 18;

10. act in violation of the first, third, fourth and fifth paragraphs of Article 19;

11. take personal data out of the country in violation of the provisions of Articles 24.

The responsible person of a legal entity shall be fined between SIT 50,000 and 100,000 under the preceding paragraph for an offence from the preceding paragraph.

The responsible person at a state body or local community body who has committed an offence from the first paragraph shall be fined between SIT 50,000 and 100,000.

Article 31

A user of data, a legal entity or an individual shall be fined between SIT 500,000 and 1,000,000 for committing an offence in the course of the independent performance of an activity if they process personal data for purposes not determined by law or in the written consent of the individual, or use it in a manner incompatible with these purposes.

A fine of between SIT 50,000 and 100,000 shall be imposed on the responsible person at the legal entity if he commits an offence from the preceding paragraph.

A fine of between SIT 50,000 and 100,000 shall be imposed on the responsible person at a state body or local community body if he commits an offence from the first paragraph of this Article.

A fine of between SIT 50,000 and 100,000 shall be imposed on an individual if he commits an offence from the first paragraph of this Article.

Article 32

A legal entity or natural person who, in the course of the independent performance of an activity, violates the authorisations contained in a contract from the second paragraph of Article 7 shall be fined between SIT 500,000 and 1,000,000.

The responsible officer of a legal person who commits an offence under the preceding paragraph shall be fined between SIT 50,000 and 100,000.

Article 33

A legal entity or individual who, in the course of the independent performance of an activity, processes personal data in keeping with this Act but fails to ensure personal data protection shall be fined between SIT 500,000 and 1,000,000 (Article 14).

The responsible person at a legal entity shall be fined between SIT 5,000 and 100,000 if he commits an offence from the preceding paragraph.

The responsible person at a state body or local community body shall be fined between SIT 50,000 and 100,000 if he commits an offence from the first paragraph of this Article.

Article 34

The person responsible for keeping and maintaining the catalogue of databases at the ministry shall be fined between SIT 50,000 and 100,000 if he violates the right of the individual to access the catalogue of databases, or does not permit him to copy data from the catalogue (Article 17).

12. Transitional and final provisions ➦

Article 35

State bodies and local community bodies, organisations and individuals performing a public service and holders of public authorisations shall bring the processing of personal data in line with the provisions of this Act within two years of its entry into force at the latest.

Article 36

On the day this Act enters into force, the following shall cease to apply:

- the provisions of the Personal Data Protection Act (Zakon o varstvo osebnih podatkov, Ur.l. RS, 8/90 and 19/91),

- provisions of the Social Information System Act (Zakon of druÏbenem sistemu informiranja, Ur.l. SRS, 10/83).

Article 37

This Act shall enter into force on the 15th day after its publication in the Official Gazette of the Republic of Slovenia.