4690. Personal Data Protection Act (official consolidated text)

(ZVOP-1-UPB1), page 12707.

On the basis of Article 153 of the Rules of Procedure of the National Assembly, at the session of 27 September 2007 the National Assembly of the Republic of Slovenia approved the official consolidated text of the Personal Data Protection Act, which includes:

- Act on the Protection of Personal Data - ZVOP-1 (Official Gazette of the Republic of Slovenia, No. 86/04 of 5 August 2004),

- Act on Information Commissioner - ZInfP (Official Gazette of the Republic of Slovenia, No. 113/05 of 16 April 2004) 12. 2005),

- Act Amending the Constitutional Court Act - ZUstS-A (Official Gazette of the Republic of Slovenia, No. 51/07 of 8.06.2007) and

- Act Amending the Personal Data Protection Act - ZVOP-1A (Official Gazette of the Republic of Slovenia, No. 67/07 of 27.7.2007).

No. 210-01 / 89-3 / 33

Ljubljana, September 27, 2007

EPA 1584-IV

President of the

National Assembly of the Republic of Slovenia

France Cukjati, Med., Lr

LAW

ON PROTECTION OF PERSONAL DATA official consolidated text (ZVOP-1-UPB1)

PART I

GENERAL PROVISIONS

Content of the law

Article 1

This law defines the rights, obligations, principles and measures to prevent unconstitutional, unlawful and unjustified interference with the privacy and dignity of an individual or individual (hereinafter: an individual) in the processing of personal data.

Principle of legality and fairness

Article 2

Personal data is processed legally and fairly.

Principle of proportionality

Article 3

The personal data processed must be appropriate and to the extent appropriate for the purposes for which they are collected and further processed.

Prohibition of discrimination

Article 4

Protection of personal data is guaranteed to every individual irrespective of nationality, race, color, religion, ethnicity, gender, language, political or other belief, sexual orientation, wealth, birth, education, social status, citizenship, place or type of residence, or Any other personal circumstance.

Territorial validity of this Act

Article 5

(1) This Act applies to the processing of personal data if the data controller is established, registered or registered in the Republic of Slovenia or if the branch of the personal data controller is registered in the Republic of Slovenia.

(2) This Act shall also apply if the data controller is not established, is not established or is not registered in a Member State of the European Union or is not part of the European Economic Area and uses automated or other equipment located in the Republic of Slovenia for the

processing of personal data If this equipment is used only for the transfer of personal data through the territory of the Republic of Slovenia.

(3) The controller of personal data referred to in the preceding paragraph shall determine the natural or legal person established or registered in the Republic of Slovenia, which he represents with regard to the processing of personal data in accordance with this Act.

(4) This Act shall also apply to diplomatic, consular and other official representations of the Republic of Slovenia abroad.

The meaning of the terms

Article 6

The terms used in this Act shall have the following meanings:

1. Personal information - is any information that refers to an individual, regardless of the form in which it is expressed.

2. Individual - is a defined or identifiable natural person to whom the personal data relates; A natural person is identifiable if it can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors characterizing his physical, physiological, mental, economic, cultural or social identity, the method of identification being Causes great costs, disproportionately high effort or does not require much time.

3. Processing of personal data - means any operation or set of operations which is carried out in relation to personal data which have been automated or which are part of a personal data collection database or are intended to be included in a personal data file, in particular the collection, Subscribing, editing, storing, adjusting or modifying, invoking, inspecting, using, disclosing by transmission, communicating, disseminating or otherwise making available, sorting or linking, blocking, anonymizing, deleting or destroying; Processing may be manual or automated (processing means).

4. Automated processing - the processing of personal data by means of information technology.

5. Personal data collection - any structured data set containing at least one personal data that is accessible on the basis of criteria that allow the use or aggregation of data, regardless of whether the set is centralized, decentralized or dispersed in a functional or geographical Basis; A structured data set is a set of data that is organized in such a way as to determine or enable the individual's determination.

6. The personal data controller shall be a natural or legal person or other person of the public or private sector who, alone or jointly with others, determines the purposes and means of processing personal data or a person designated by law, which also determines the purposes and means of processing.

7. Contractor - is a natural or legal person who processes personal data in the name and on behalf of the data controller.

8. The user of personal data - is a natural or legal person or other person of the public or private sector to whom the personal data are transmitted or disclosed.

9. Transmission of personal data - the transmission or disclosure of personal data.

10. A foreign user and a foreign data controller - is a user of personal data in a third country and a data controller in a third country.

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

12. The catalog of the personal data collection - is a description of the personal data collection.

13. Register of personal data collections - a register containing data from catalogs of personal data collections.

14. Individual consent of an individual - is a voluntary statement of the will of the individual that his personal data may be processed for a specific purpose and is given on the basis of the information which the manager must provide to him under this Act; Personal consent of the individual can be written, oral or other appropriate consent of the individual.

15. Written consent of an individual - the consent of an individual who has the form of a charter, provisions in the contract, provisions in the contract, annexes to the application or other form in accordance with the law is signed; On the basis of a signed bill, the signature is also a uniform format given by a telecommunication means, and on the basis of a signed law, a uniform format given by an individual who does not know or can not write.

16. Oral or other appropriate consent of the individual - it is an oral or telecommunication or other appropriate means or otherwise appropriately given consent from which it is possible to conclude on the individual's consent.

17. Blocking - this is the marking of personal data to restrict or prevent further processing.

18. Anonymisation - this is a change in the form of personal data so that it can no longer be linked to an individual, or is only possible with disproportionately large efforts, costs or time consumption.

19. Sensitive personal data - data on racial, national or ethnic origin, political, religious or philosophical beliefs, trade union membership, health status, sexual life, registration or erasure in or from criminal records or records kept under the law , Which regulates misdemeanors (hereinafter: misdemeanor records); Sensitive personal data are also biometric characteristics if their use can be determined by an individual in relation to any of the above circumstances.

20. The same connecting signs - the personal identification number and others are uniquely identifiable by the law of the individual, by means of which it is possible to collect or retrieve personal data from those collections of personal data in which the same connecting signs are processed.

21. Biometric features - these are the physical, physiological and behavioral characteristics that all individuals have, but are unique and permanent for each individual, and it is possible to identify the individual, in particular by using a fingerprint, a clip of papyrus lines from the finger, the iris , Eye retina, face, ears, deoxyribonucleic acid and typical postures.

22. The public sector - are state bodies, local self-governance bodies, holders of public authority, public agencies, public funds, public institutions, universities, independent higher education institutions and self-governing national communities.

23. Private sector - are legal entities and natural persons performing activities under the law governing companies or public utilities or trades, and persons of private law; Private sector are public economic institutions, public companies and companies irrespective of the share or influence of the state, self-governing local community or self-governing national community.

Exceptions to the application of this Act

Article 7

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

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

(3) For the personal data processed by the media for the purposes of informing the public, the second paragraph of Article 25, paragraphs 26, 27 and 28 and part one of this Act shall not apply.

(4) Data controllers with fewer than 50 employees shall not be required to fulfill the obligations referred to in the second paragraph of Article 25 and the obligations referred to in Articles 26 and 27 of this Act.

(5) The exceptions referred to in the preceding paragraph shall not apply to personal data collections managed by public sector personal data managers, notaries, lawyers, detectives, executors, private security providers, private health professionals, providers of health services and personal data controllers, Which keep collections containing sensitive personal information and the processing of sensitive personal data is part of their registered activity.

II. PART
TREATMENT OF PERSONAL DATA
Chapter 1
Legal bases and purposes
General definition
Article 8

(1) Personal data may only be processed if the processing of personal data and personal data being processed is determined by law or if the personal consent of the individual is made for the processing of certain personal data.

(2) The purpose of the processing of personal data must be laid down in the law, and in the case of processing on the basis of the personal consent of an individual, the individual must be informed in advance in writing or in another appropriate manner of the purpose of the processing of personal data.

Legal bases in the public sector
Article 9

(1) Personal data in the public sector may be processed if the processing of personal data and personal data being processed is determined by law. The law may stipulate that certain personal data are processed solely on the basis of the personal consent of the individual.

(2) Public authorizations may also process personal data also on the basis of the personal consent of the individual without a basis in the law, when it is not about the exercise of their duties as holders of public authorizations. Collection of personal data generated on this basis must be separate from the collections of personal data that arise from the exercise of the tasks of the holder of public authority.

(3) Notwithstanding the first paragraph of this article, the personal data of individuals who have concluded a contract with the public sector or who are on the basis of the initiative of an individual with him during the negotiation phase for the conclusion of a contract may be processed in the public sector if the processing of personal data is necessary and Suitable for carrying out negotiations to conclude a contract or to fulfill a contract.

(4) Notwithstanding the first paragraph of this article, personal data that are necessary for the exercise of legal powers, duties or obligations of the public sector may exceptionally be processed in the public sector if such processing does not interfere with the legitimate interest of the individual to whom Personal data relate.

Legal bases in the private sector

Article 10

(1) Personal data in the private sector may be processed if the processing of personal data and personal data processed is determined by the law or if the personal consent of the individual is given for the processing of certain personal data.

(2) Notwithstanding the preceding paragraph, private data may be processed in the private sector by individuals who have entered into a contract with the private sector or are on the basis of an individual's initiative in the negotiation phase for the conclusion of the contract if the processing of personal data is necessary and appropriate for Conducting negotiations for the conclusion of a contract or for fulfilling the contract.

(3) Notwithstanding the first paragraph of this article, personal data may be processed in the private sector if this is necessary for the purpose of pursuing the legitimate interests of the private sector and these interests clearly prevail over the interests of the data subject.

Contract processing

Article 11

(1) The personal data controller may entrust individual tasks with regard to the processing of personal data to the contractor who is registered to perform such an activity and provides the appropriate procedures and measures referred to in Article 24 of this Act.

(2) A contractual processor may carry out individual tasks relating to the processing of personal data within the framework of the client's authority and may not process personal data for any other purpose. Mutual rights and obligations shall be regulated by a contract that must be concluded in writing and include an agreement on the procedures and measures referred to in Article 24 of this Act. The controller of personal data shall supervise the implementation of the procedures and measures referred to in Article 24 of this Act.

(3) In the event of a dispute between the data controller and the contractor, the contractor shall, on the basis of the request of the controller, confidently return the personal data which he has contracted to the controller. Any copies of this information must be immediately destroyed or forwarded to a state body which, in accordance with the law, is competent to detect or prosecute criminal offenses, to the court or other state authority, if so provided by the law.

(4) In the event of termination of the contractor, personal data shall be returned to the data controller without undue delay.

Protecting the vital interests of the individual

Article 12

If the processing of personal data is indispensable for the protection of a person's life or body, his personal data may be processed notwithstanding that there is no other legitimate legal basis for processing this information.

Processing sensitive personal data

Article 13

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

1. if the individual has given express personal consent for this, which is, as a rule, written and in the public sector also determined by law;

2. if processing is necessary in order to fulfill the obligations and special rights of the data controller in the field of employment in accordance with the law, which also provides appropriate guarantees for the rights of the individual;

3. if processing is indispensable for the protection of the life or body of the data subject or of other persons when the data subject is physically or commercially unable to give his consent referred to in point 1 of this Article;

4. if they are processed by institutions, associations, societies, religious communities, trade unions or other non-profit organizations for political, philosophical, religious or trade-union purposes for the purposes of legal activities, but only if the treatment relates to their members or to individuals who are in In relation to these objectives, with them in regular contact, and if such information is not transmitted to other individuals or persons in the public or private sector without the written consent of the individual to whom they relate;

5. if the individual to whom sensitive personal data relate publicly discloses it without obvious or explicit intention to limit the purpose of their use;

6. if they are processed by healthcare professionals and medical staff for the purposes of health care for the population and individuals and the management or provision of health services in accordance with the law;

7. if necessary for the purpose of enforcing or opposing the legal claim;

8. if so provided by another law for the purpose of exercising the public interest.

Securing sensitive personal information

Article 14

(1) Sensitive personal data must be specifically marked and protected in the process so that unauthorized persons are denied access to them, except in the case referred to in point 5 of Article 13 of this Act.

(2) When transferring sensitive personal data through telecommunication networks, data are considered to be adequately protected, provided that they are transmitted using cryptographic methods and electronic signatures in such a way as to ensure their unreadability or unrecognizability during transmission.

Automated decision making

Article 15

Automated processing of personal data in which an individual may be subject to a decision which results in or has significant effects on or in connection with legal effects, and which is based solely on the automated processing of data intended to evaluate certain personal aspects relating thereto, Such as its performance at work, creditworthiness, reliability, compliance or compliance with the required conditions, is permitted only if the decision is:

1. accepted during the conclusion or implementation of the contract, provided that the initiative for the conclusion or implementation of the contract submitted by the data subject is fulfilled or that there are appropriate measures to protect his legitimate interests, such as, in particular, arrangements , Which enable him to object to such a decision or to express his position;

2. determined by law, which also provides measures for the protection of the legitimate interests of the data subject, in particular the possibility of a legal remedy against such a decision.

The purpose of collection and further processing

Article 16

Personal data may be collected only for specified and lawful purposes and may not be further processed in such a way that their processing would be inconsistent with these purposes unless otherwise provided by the law.

Treatment for historical, statistical and scientific research purposes

Article 17

(1) Notwithstanding the original purpose of the collection, personal data may be further processed for historical, statistical and scientific research purposes.

(2) Personal data shall be transmitted to the user of personal data for the purpose of the processing referred to in the preceding paragraph in an anonymous form, unless otherwise provided by the law or if the data subject has not previously provided written consent for processing without anonymisation.

(3) The personal data transmitted to the user of personal data in accordance with the preceding paragraph shall be destroyed at the end of the processing, unless otherwise provided by the law. The user of personal data must inform the data controller who provided his personal data in writing, without delay, after their destruction, when and in what manner he destroyed them.

(4) The results of the processing referred to in the first paragraph of this Article shall be published in an anonymous form, unless the law provides otherwise or if the data subject has given written consent for publication in a non-anonymous form or if written consent is given for such publication Heirs of the deceased person under this Act.

Chapter 2
Protection of individuals
Accuracy and promptness of personal data
Article 18

(1) Personal data to be processed must be accurate and up to date.

(2) Before entering the personal data database, the data controller may verify the accuracy of personal information by inspecting the identity document or other relevant public document of the individual to whom it relates.

Informing an individual about the processing of personal data
Article 19

(1) If personal data are collected directly from the individual to whom it relates, the data controller or his representative must communicate the following information to an individual if the individual is not yet acquainted with them:

- information about the data controller and his / her possible representative (personal name , Name or firm and address or registered office),

- purpose of processing personal data.

(2) In relation to the specific circumstances of collecting personal data from the previous paragraph need to ensure lawful and fair processing of personal data of an individual, the person referred to in the preceding paragraph shall communicate to the individual additional information,

if the person with them is not yet aware of, in particular:

- An indication of the user or the type of users of his personal information,

- the indication whether the collection of personal data is compulsory or voluntary, and the

possible consequences if it does not provide voluntary data;

- information on the right to inspect, copy, copy, update, correct, block and delete personal data relating to it.

(3) If personal data were not collected directly from the individual to whom it relates, the data controller or his representative must provide the following information at the latest at the time of entry or transmission of personal data to the data subject:

- the data on the data controller and his / her possible representative (Personal name, name or firm and address or registered office),

- purpose of processing personal data.

(4) In relation to the specific circumstances of collecting personal data from the previous paragraph need to ensure lawful and fair processing of personal data of an individual, the person referred to in the preceding paragraph shall communicate to the individual additional information, in particular:

- information on the nature of the personal data collected

- An indication of the user or the type of users of his personal information,

- information on the right to inspect, copy, copy, update, correct, block and delete personal data relating to him.

(5) It is not necessary to provide the information referred to in the third and fourth paragraphs of this Article if it would be impossible or would cause significant costs for the purpose of processing personal data for historical, statistical or scientific research purposes, disproportionately high effort or requiring a lot of time or if The law expressly specifies the entry or transmission of personal data.

Use the same connecting sign

Article 20

(1) In the collection of personal data from collections of personal data in the field of health, the police, intelligence and security activities of the state, the defense of the state, the judiciary and the state prosecutor's office and criminal records and misdemeanor records, it is not permitted to use the same connecting sign in such a way that, Personal data used only that character.

(2) Notwithstanding the preceding paragraph, the same link for obtaining personal data may exceptionally be used, provided that this is the only information in a specific case which may enable the offense to be discovered or prosecuted ex officio to protect the life or the body An individual, or to ensure that the tasks of the intelligence and security authorities are laid down by law. An official endorsement or other written record must be made without delay.

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

Deadline for the 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) After completion of the purpose of the processing, personal data are deleted, destroyed, blocked or anonymised, if they are not defined by the law governing archives and archives as archival material, or if the law does not specify otherwise for individual types of personal data.

Transmission of personal data

Article 22

(1) The data controller must, in the absence of a law, provide personal data to users of personal data against payment of the costs of transmission.

(2) The administrator of the central population register or records of permanent residents and temporary residents must forward to the beneficiary in the manner specified for the issue of the certificate, showing the legal interest in exercising rights before public sector entities, the personal name and address of the permanent or temporary residence of the individual, Against which he exercises his rights.

(3) For each transmission of personal data, the data controller must ensure that it is possible to determine later what personal data have been transmitted, to whom, when and on what basis,

for the period during which the legal protection of the individual's right to act in an unlawful manner Personal information.

(4) Notwithstanding the first paragraph of this Article, the public sector personal data controller shall provide personal data to the user in the public sector with personal data without payment of mediation costs, unless the law provides otherwise or if it is a use for historical, statistical or scientific research Purpose.

Protection of personal data of deceased individuals

Article 23

(1) The data controller may only provide information to the deceased person only to those users of personal data who are empowered by law to process personal data.

(2) Notwithstanding the preceding paragraph, the data controller shall forward the information to the deceased person to a person who, according to the law governing the inheritance, is his legal heir of the first or second order of succession, if the use of personal data proves a legal interest, and the deceased is not in writing Prohibited the transmission of such personal data.

(3) Unless the law provides otherwise, the data controller may also transmit the data referred to in the preceding paragraph to any other person who intends to use these data for historical, statistical or scientific research purposes, if the deceased person did not prohibit the transmission of such personal data in writing.

(4) If the deceased individual did not submit the prohibition referred to in the preceding paragraph, persons who, according to the law governing the inheritance, may be legally hedgeers of the first or second order of law, shall be prohibited in writing in the transmission of his data unless otherwise provided by the law.

Chapter 3

Personal Data Protection

Content

Article 24

(1) Personal data protection shall include organizational, technical and logical technical procedures and measures protecting personal data, prevent accidental or deliberate unauthorized destruction of data, their alteration or loss, and unauthorized processing of such data by:

1. protecting Premises, equipment and system software, including input / output units;

2. Protects the application software for processing personal data;

3. prevents unauthorized access to personal data when transmitted, including transmission by telecommunications and networks;

4. provides an effective way of blocking, destroying, erasing or anonymizing personal data;

5. allows the subsequent determination of the date when individual personal data were entered into the personal data database, used or otherwise processed and who did it for the period during which the legal protection of the individual's right for the inadmissible transmission or processing of personal data is possible.

(2) In the case of the processing of personal data accessible through a telecommunications device or network, the hardware, system and application software must ensure that the processing of personal data in the personal data collections is within the limits of the personal data of the user.

(3) Procedures and measures for the protection of personal data must be appropriate in the light of the risks posed by the processing and the nature of the particular personal data being processed.

(4) Officials, employees and other individuals performing duties or tasks in persons who process personal data shall be obliged to protect the confidentiality of personal data that they acquire in the performance of their functions, duties and duties. The obligation to protect the confidentiality of personal data is also binding on them after the termination of office, employment, performance of duties or the provision of contractual processing services.

The obligation to insure

Article 25

(1) Data controllers and contractual processors shall be obliged to provide personal data protection in the manner referred to in Article 24 of this Act.

(2) The personal data controllers shall prescribe in their acts the procedures and measures for the protection of personal data and determine the persons responsible for certain personal data collections and persons who, due to the nature of their work, may process certain personal data.

Chapter 4

Information about personal data collections

Catalog of personal data collection

Article 26

(1) The data controller shall set up a personal data collection catalog for each database of personal data, which shall include:

1. the name of the personal data collection;

2. data on the personal data controller (for a natural person: personal name, address of activity or address of permanent or temporary residence, and for a sole proprietor of an individual, a name, registered office and registration number, for a legal entity: name or company name and address of the manager Personal data and registration number);

3. the legal basis for the processing of personal data;

4. categories of data subjects;

5. types of personal data in the personal data collection;

6. the purpose of the treatment;

7. the period of retention of personal data;

8. Restrictions on the rights of individuals with regard to personal data in the Personal Data Base and the legal basis of the restrictions;

9. users or categories of users of personal data contained in the personal data collection;

10. the fact that personal data are transferred to a third country, where, to whom and the legal basis of the amount;

11. a general description of personal data protection;

12. data on related personal data collections from official records and public books;

13. information on the representative referred to in the third paragraph of Article 5 of this Act (for a natural person: personal name, address of activity or address of permanent or temporary residence, and for sole proprietor of an individual also name, head office and registration number; Company name and address or registered office of head of personal data and registration number).

(2) The data controller must ensure the accuracy and promptness of the contents of the catalog.

Notification of the supervisory authority

Article 27

(1) The data controller shall forward the data referred to in points 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 Authority for the Protection of personal data for at least 15 days prior to the establishment of a personal data set or before entering a new type of personal data.

(2) The data controller shall transmit to the National Supervisory Body for Personal Data Protection the changes in the data referred to in the previous paragraph no later than eight days from the date of the change.

Register

Article 28

(1) The National Supervisory Authority for the protection of personal data shall keep and maintain a register of personal data collections containing data referred to in Article 27 of this Act in the manner determined by the methodology of its management.

(2) The register shall be managed by means of information technology and published on the website of the National Supervisory Authority for the Protection of Personal Data (hereinafter: the website).

(3) The rules on the methodology referred to in the first paragraph of this Article shall be determined by the minister in charge of justice, upon the proposal of the chief state supervisor or the chief state inspector for personal data protection (hereinafter: the chief state supervisor).

III. PART

RIGHTS OF THE INDIVIDUAL

Insights into the register

Article 29

(1) The national supervisory authority for the protection of personal data must allow anyone access to the register of personal data collections and the transcript of data.

(2) The insight and transcription of data must be allowed and enabled as a rule on the same day, and at the latest within eight days, otherwise the request is deemed to be rejected.

The right of the individual to acquaintance

Article 30

(1) The data controller must, at his request,

provide an individual: 1. to provide access to the catalog of the personal data collection;

2. confirm whether data are processed in respect of it or not and to enable it to inspect and process personal data contained in the personal data database and to copy or copy them;

3. to provide the display of personal data contained in the personal data database and relating to it;

4. provide a list of users to whom personal data have been transmitted, when, on what basis and for what purpose;

5. provide information on the sources on which the records on the individual contained in the personal data database and the processing method are based;

6. provide information on the purpose of the processing and the type of personal data being processed and any necessary explanations in this respect;

7. clarify the technical or logical-technical decision-making process if it carries out automated decision-making by processing personal data of an individual.

(2) The copy referred to in point 3 of the preceding paragraph shall not replace the document or certificate in accordance with the administrative or other procedure, which shall be indicated on the printout.

The process of getting acquainted

Article 31

(1) The request referred to in Article 30 of this Act shall be filed in writing or orally on the record with the data controller. The request may be lodged once every three months, with regard to the processing of sensitive personal data and personal data under the provisions of Chapter 2, Chapter 2. Part of this law once a month. Where this is necessary to ensure fair, lawful or proportionate processing of personal data, in particular where personal data of an individual in a personal data collection are often updated or transmitted or could be frequently updated or transmitted to users of personal data, the data controller must enable an individual to submit Request also within a shorter period of time which is not shorter than five days from the date of acquaintance with personal data relating to him or the rejection of this acquaintance.

(2) The data controller shall enable the individual to inspect, copy, copy and certify according to points 1 and 2 of the first paragraph of Article 30 of this Act, as a rule, on the same day as the day the request was received, and at the latest within 15 days, or in 15 Days to notify in writing the reasons why they will not be able to view, copy, copy or issue the certificate.

(3) The excerpt from point 3, the list from point 4, the information from points 5 and 6 and the explanation from point 7 of the first paragraph of Article 30 of this Act must be transmitted by the data controller to the individual within 30 days of the day when Received the request, or within the same time limit, inform him in writing of the reasons why he would not forward his printout, list, information or explanation to him.

(4) If the operator fails to act in accordance with the second and third paragraphs of this Article, the request shall be deemed to be rejected.

(5) The costs relating to the request and consultation referred to in this Article shall be borne by the data controller.

(6) For copying, copying and a written confirmation in accordance with point 2 and for the extract from item 3, the list from point 4, the information from points 5 and 6 and the explanation from point 7 of the first paragraph of Article 30 of this Act The personal data controller only charges the individual with material costs according to a predetermined price list, in that the oral verification in accordance with point 2, oral information under item 5, oral information under item 6 and oral explanation under item 7 are free of charge. If an individual, in spite of obtaining oral certificates, information or explanations in accordance with points 2, 5, 6 and 7 of the first paragraph of Article

30 of this Act, requires a certificate, information or explanation in writing, the data controller must provide this information.

(7) On the basis of the proposal of the Information Commissioner, the minister responsible for justice shall prescribe the price list for the material costs referred to in the preceding paragraph and shall publish it in the Official Gazette of the Republic of Slovenia.

Right to supplement, repair, block, erase and objection

Article 32

(1) At the request of the data subject, the data controller must complete, repair, block or delete personal data for which an individual proves to be incomplete, inaccurate or non-aggressive, or that they have been collected or processed contrary to Law.

(2) At the request of an individual, the data controller shall, at the request of an individual, inform all users of personal data and contractual processors to whom he transmitted individual personal data before the measures referred to in the preceding paragraph have been carried out, on their completion, correction, blocking or erasure under the preceding paragraph. Exceptionally, it does not have to do this if it would cause great costs, disproportionately great effort, or require a lot of time.

(3) An individual 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 at any time have the right to demand the termination of their processing by an objection. The controller shall grant the objection if the individual proves that the conditions for processing under the fourth paragraph of Article 9 or the third paragraph of Article 10 of this Act are not met. In this case, his personal data may no longer be processed.

(4) If the controller fails to satisfy the objection referred to in the preceding paragraph, the individual who has filed the objection may request that the State Supervisory Authority for the protection of personal data decide on the processing in accordance with the fourth paragraph of Article 9 or the third paragraph of Article 10 of this Act. An individual may file a request within seven days of the delivery of the decision on the objection.

(5) The National Supervisory Authority for the Protection of Personal Data shall decide on the request referred to in the preceding paragraph within two months of receipt of the request. The filed request shall withhold the processing of the personal data of the individual in respect of which the request was made.

(6) The costs of all acts of the data controller referred to in the preceding paragraphs shall be borne by the controller.

Procedure for replenishment, repair, blocking, deletion, and objection

Article 33

(1) The request or objection referred to in Article 32 of this Act shall be filed in writing or orally on the record with the personal data controller.

(2) The personal data controller must complete, update, block, delete or delete personal data within 15 days from the date on which he received the request and inform the applicant of the request or inform him within the same time limit of the reasons why he would not do so. Within the same time limit, it must decide on the objection.

(3) If the personal data controller does not comply with the previous paragraph, the request shall be deemed to be rejected.

(4) If the personal data controller itself finds that personal data are incomplete, inaccurate or not accurate, they supplement or correct them and inform the individual thereof, unless otherwise provided by the law.

(5) The costs relating to the updating, correction and deletion of personal data, communications and the decision on opposition shall be borne by the data controller.

Judicial protection of the rights of the individual

Article 34

(1) An individual who finds that his rights as defined by this Act have been violated may request judicial protection throughout the infringement.

(2) If the violation referred to in the preceding paragraph has ceased, an individual may file an action for the purpose of finding that the violation existed, provided that no other judicial protection is provided for him in connection with the violation.

(3) The competent court shall decide in the procedure according to the provisions of the law governing administrative dispute, unless otherwise provided by this law.

(4) In the procedure, the public is excluded if the court does not decide otherwise on the proposal of the individual for justified reasons.

(5) The procedure is necessary and preferred.

Temporary injunction

Article 35

In an application filed for violation of the rights referred to in Article 32 of this Act, an individual may request from the court to order a final decision in an administrative dispute to the data controller to prevent any processing of the personal data in question if the person concerned was affected by their processing And the delay in processing does not preclude public benefit and there is also no risk of a greater irreparable damage to the counterparty.

Limitation of individual rights

Article 36

(1) The rights of an individual referred to in the third and fourth paragraphs of Article 19, Articles 30 and 32 of this Act may exceptionally be limited by law for reasons of the protection of the sovereignty and defense of the state, the protection of national security and the constitutional organization of the state, security, political and economic interests States, the exercise of police powers, the prevention, disclosure, detection, proving and prosecution of criminal offenses and offenses, the detection and punishment of violations of ethical standards for certain professions, for monetary, budgetary or tax purposes, for the purpose of overseeing the police and the protection of the individual to whom they relate Personal data, or the rights and freedoms of others.

(2) The restrictions referred to in the preceding paragraph may be determined only to the extent necessary to achieve the purpose for which the restriction is determined.

IV. PART
INSTITUTIONAL PROTECTION OF PERSONAL DATA
Chapter 1
Supervisory Authority for the Protection of Personal Data
Supervisory Authority
Article 37

(1) The national supervisory authority for the protection of personal data (hereinafter: the national supervisory authority) shall have the status of the supervisory authority for the protection of personal data.

(2) The national supervisory authority shall carry out an inspection of the implementation of the provisions of this Act and other tasks under this Act and other regulations governing the protection or processing of personal data or the amount of personal data from the Republic of Slovenia. The National Supervisory Authority also performs other tasks in accordance with the law.

(3) The national supervisory authority shall ensure the uniform implementation of measures in the field of the protection of personal data.

Position and organization of the national supervisory authority
Article 38

(Expired)

Resources for the work of the national supervisory authority
Article 39

(Expired)

Appointment of the Chief State Supervisor
Article 40

(Ceased to bend)

Dismissal of the Chief State Supervisor
Article 41

(Expired)

Replacement of the Chief State Supervisor
Article 42

(Expired)

Supervisor

Article 43

(Expired)

Independence of supervisors

Article 44

(Expired)

Jobs and assignments to the national supervisory authority

Article 45

(Expired)

Chapter 2

The tasks of the national supervisory authority

Reports of the national supervisory authority

Article 46

(Expired)

Cooperation with other authorities

Article 47

In its work, the National Supervisory Authority cooperates with the national authorities, the competent bodies of the European Union for the protection of individuals with regard to the processing of personal data, international organizations, foreign personal data protection supervisors, institutes, associations, non-governmental organizations in the field of personal data protection or privacy and other organizations And authorities on all issues of relevance to the protection of personal data.

Regulatory powers

Article 48

(1) The National Supervisory Authority shall give preliminary opinions to the ministries, the National Assembly, the bodies of self-governing local communities, other state bodies and holders of public authorizations on the harmonization of the provisions of draft laws and other regulations with laws and other regulations governing personal data.

(2) (ceases to apply)

Publicity work

Article 49

(1) The national supervisory authority may:

1. issue an internal newsletter and professional literature;

2. publish on the website or in another appropriate manner the preliminary opinions referred to in the first paragraph of Article 48 of this Act after the law or other regulation has been adopted and published in the Official Gazette of the Republic of Slovenia, in the bulletin of a self-governing local community or published in another lawful manner ;

3. publishes the requests referred to in the second paragraph of Article 48 of this Act on the website or in another appropriate manner after receiving them by the Constitutional Court;

4. publish on the website or other appropriate manner the decisions and decisions of the Constitutional Court on the requirements referred to in the second paragraph of Article 48 of this Act;

5. publishes decisions and decisions of courts with general jurisdiction and administrative court regarding the protection of personal data on a website or other appropriate way, so that it is not possible to disclose personal data of clients, victims, witnesses or experts;

6. gives optional opinions on the compliance of codes of professional ethics, general conditions of business or their proposals with regulations in the field of personal data protection;

7. Provides non-mandatory opinions, clarifications and views on personal data protection issues and publishes them on a website or in another appropriate manner;

8. prepares and gives optional instructions and recommendations regarding the protection of personal data in a particular field;

9. makes public statements about the inspections carried out in individual cases;

10. conducts press conferences on the work of the national supervisory authority and makes copies of declarations or recordings of press releases from press conferences on the website;

11. publishes other important notices on the website.

(2) The National Supervisory Authority may invite representatives of associations and other non-governmental organizations in the field of protection of personal data, privacy and consumers to engage in competencies from points 6, 7 and 8 of the previous paragraph.

Chapter 3

Inspection

Application of the law governing inspection

Article 50

For the purpose of performing inspection under this Act, the provisions of the Act governing inspection shall apply, unless otherwise provided by this Act.

Scope of inspection

Article 51

In the framework of inspection supervision, the national supervisory authority shall:

1. supervise the legality of the processing of personal data;

2. supervises the appropriateness of measures for the protection of personal data and the implementation of procedures and measures for the protection of personal data under Articles 24 and 25 of this Act;

3. supervise the implementation of the provisions of the Act governing the catalog of the personal data collection, the register of personal data collections and the recording of the transmission of personal data to individual users of personal data;

4. supervise the implementation of the provisions of the law regarding the export of personal data to a third country and their transmission to foreign users of personal data.

Direct inspection

Article 52

(1) Inspection supervision shall be carried out directly by the supervisor within the limits of the powers of the national supervisory authority.

(2) The supervisor shall be empowered to perform inspection tasks with an official card containing a photograph of the supervisor, his personal name, professional or scientific address and other necessary information. The form and content of the service card shall be prescribed in detail by the minister responsible for justice.

Supervisor's powers

Article 53

In performing the inspection, the supervisor is entitled to:

1. review the documentation relating to the processing of personal data, regardless of its confidentiality or secrecy, and the transfer of personal data to a third country and the transmission to third parties of personal data;

2. review the contents of personal data collections, regardless of their confidentiality or confidentiality and catalogs of personal data collections;

3. review the documentation and acts governing the protection of personal data;

4. to inspect the premises in which personal data, computer and other equipment and technical documentation are processed;

5. to check the measures and procedures for securing personal data and their implementation;

6. to exercise other powers provided for by the law governing inspection and by the law governing the general administrative procedure;

7. to perform other matters determined by law.

Inspection measures

Article 54

(1) A supervisor who establishes a violation of this Act or other law or regulation governing the protection of personal data when performing inspection, shall have the right immediately:

1. to order that the irregularities or defects identified by them be eliminated in the manner and within the time limit , Which he himself determines;

2. order the prohibition of the processing of personal data by persons in the public or private sector who have not provided or are not implementing personal data protection measures and procedures;

3. order the prohibition of the processing of personal data and the anonymisation, blocking, erasure or destruction of personal data when it finds that personal data is processed in contravention of the provisions of the law;

4. order the prohibition of the transfer of personal data to a third country or their transmission to foreign users of personal data if they are disclosed or transmitted contrary to the provisions of a law or a binding international treaty;

5. order other measures laid down by the act governing inspection and by the law governing the general administrative procedure.

(2) The measures referred to in the preceding paragraph can not be ordered against a person who provides data transmission services in the electronic communications network, including temporary storage of data and other activities in relation to data that are predominantly or fully in the function of facilitating or facilitating the transmission of data by Networks, if that person does not have an interest in himself relating to the content of this information, and is not a person who can effectively control access to this data alone or with a limited circle of persons associated with it.

(3) If the supervisor finds, during inspection, that there is a suspicion of committing a criminal offense, or a misdemeanor shall submit a criminal report or carry out procedures in accordance with the law regulating misdemeanors.

Judicial protection

Article 55

There is no appeal against the decision or decision of the supervisor referred to in the first paragraph of Article 54 of this Act and administrative dispute is permitted.

Informing the applicant

Article 56

The supervisor is obliged to inform the applicant of all important findings and actions in the procedure of inspection supervision.

Responsibilities of the national supervisory authority regarding access to public information

Article 57

(Expired)

Secrecy

Article 58

(1) The supervisor shall be obliged to protect the confidentiality of personal data, which he / she acquainted with in the course of the inspection, even after the termination of the supervisor's service.

(2) The duty referred to in the preceding paragraph shall also apply to all civil servants in the national supervisory authority.

Chapter 4

Cooperation and external supervision in the field of personal data protection

Ombudsman

Article 59

(1) The Ombudsman (Ombudsman) (hereinafter referred to as the Ombudsman) performs his duties in the field of the protection of personal data in relation to state bodies, bodies of self-governing local communities and holders of public authority in accordance with the law regulating the Ombudsman.

(2) The protection of personal data is a special field of the ombudsman, for which one of the deputy ombudsmen is responsible.

Annual Report

Article 60

In his annual report, the Ombudsman reports to the National Assembly on findings, proposals and recommendations, as well as on the state of personal data protection.

The competence of the National Assembly

Article 61

The situation in the field of personal data protection and enforcement of the provisions of this law is monitored by the competent working body of the National Assembly.

PART V

AMOUNT OF PERSONAL DATA

Chapter 1

The amount of personal data in the Member States of the European Union and the European Economic Area

Free flow of personal data

Article 62

When personal data are transmitted to the data controller, the contracted processor or the user of personal data established, registered or registered in a Member State of the European Union or the European Economic Area or is otherwise subject to its legal order, the provisions of this Act The amount of personal data to third countries.

Chapter 2

The amount of personal data to third countries

General provision

Article 63

(1) The transmission of personal data processed or to be processed only after being transmitted to a third country shall be permissible in accordance with the provisions of this Act and provided that the national supervisory authority issues a decision to ensure that the country in which it is made Adequate level of protection of personal data.

(2) The decision referred to in the preceding paragraph shall not be required if the third country is on the list of those countries referred to in Article 66 of this Act, which are found to provide an adequate level of protection of personal data.

(3) The decision referred to in the first paragraph of this Article shall not be required if the third country is on the list of those countries referred to in Article 66 of this Act, which are found to provide partially the appropriate level of protection of personal data, if those personal data are transmitted and for those Purposes for which an appropriate level of protection has been established.

Procedure for determining the appropriate level of protection of personal data

Article 64

(1) The national supervisory authority shall establish a procedure for the establishment of an appropriate level of protection of personal data in a third country on the basis of the findings of

the inspection or at the request of a natural or legal person who may demonstrate a legal interest in the issuing of a decision.

(2) Upon request of the national supervisory authority, the ministry responsible for foreign affairs shall obtain the necessary information from the competent authority of the third country as to whether that country ensures an adequate level of protection of personal data.

(3) The national supervisory authority may obtain additional information on the appropriate level of protection of personal data in a third country directly from other supervisory authorities and from the competent authority of the European Union.

(4) The National Supervisory Authority shall issue a decision within two months of receiving the complete information referred to in the second and third paragraphs of this Article. The decision may also be issued only on a specific type of personal data or their processing for a specific purpose.

(5) The national supervisory authority shall be obliged to inform the competent authority of the European Union in writing not later than 15 days after the decision has been issued that the third country does not provide an adequate level of protection of personal data.

Judicial protection

Article 65

There is no appeal against the decision referred to in the fourth paragraph of Article 64 of this Act and administrative dispute is allowed.

List

Article 66

(1) The national supervisory authority shall keep a list of third countries for which it has determined that they have a full or partial guarantee of an adequate level of protection of personal data, or that they do not provide them. If it is established that a third country only partially ensures an adequate level of protection of personal data, the list shall also indicate in which part the appropriate level is assured.

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

Bondage of the national supervisory authority in deciding

Article 67

In decision making, the national supervisory authority is bound by the decisions of the competent European Union body to assess whether third countries provide an adequate level of protection of personal data.

Deciding on the amount of personal data

Article 68

(1) When deciding on the appropriate level of protection of personal data in a third country, the national supervisory authority shall be obliged to determine all the circumstances concerning the personal data. In particular, it must take into account the type of personal data, the purpose and duration of the proposed processing, the legal arrangements in the country of origin and the recipient country, including the protection of personal data of foreign nationals and the personal data protection measures applied in them.

(2) In deciding in the preceding paragraph, the national supervisory authority shall take into account in particular:

1. whether the personal data disclosed are used solely for the purpose for which they were presented, or the purpose may be changed only on the basis of the authorization of the data controller who provided it, Or on the basis of the personal consent of the data subject;

2. whether the data subject has the opportunity to find out for what purpose his personal data have been used, to whom they have been transmitted, and the possibility of correcting or erasing inaccurate or inaccurate personal data, unless this is forbidden by the procedure for secrecy International treaties;

3. whether the foreign controller implements appropriate organizational and technical procedures and measures to protect personal data;

4. whether a contact person is authorized to provide information to the data subject or to a national supervisory authority on the processing of personal data that have been brought out;

5. Can a foreign user make personal data only if he / she provides adequate protection of personal data to foreign nationals for the other foreign user to whom personal data are transmitted;

6. Whether effective legal protection is provided to individuals whose personal data have been disclosed.

Rules

Article 69

At the proposal of the Chief State Supervisor, the minister responsible for justice, with the consent of the Minister responsible for foreign affairs, issues a rulebook detailing which information is considered necessary in the decision of the state supervisory authority on the amount of personal data to third countries.

Special provisions

Article 70

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

1. this is determined by another law or binding international treaty;

2. the personal consent of the data subject and the consequences of such mediation is given;

3. the amount necessary for the fulfillment of a contract between the data subject and the data controller or for the execution of pre-contractual measures taken in response to the request of the data subject;

4. the amount needed to conclude or execute a contract for the benefit of the data subject concluded between the data controller and a third party;

5. the amount is necessary in order to protect the life or body of the data subject against serious threats;

6. the amount shall be made out of registers, public books or official records which, by law, are intended to provide information to the public and are available for public consultation in general or any person who may demonstrate a legitimate interest in the fulfillment of conditions in a particular case They are determined by law for inspection;

7. the personal data controller shall provide appropriate measures for the protection of personal data and the fundamental rights and freedoms of individuals and shall indicate the possibilities for their exercise or protection, in particular in the provisions of the Treaties or in the general conditions of business.

(2) In the event of the personal data being disclosed in accordance with point 7 of the preceding paragraph, a person who intends to transfer personal data must obtain a special decision of the state supervisory authority authorizing the amount of personal data.

(3) The person may file personal data only after receiving the decision from the previous paragraph, by which the amount is allowed.

(4) There is no appeal against the decision referred to in the second paragraph of this article, but administrative dispute is allowed. The administrative dispute procedure is a necessary and preferred one.

(5) The national supervisory authority shall, within a period of 15 days from the issuance of the decision referred to in the second paragraph of this Article, forward this to the competent body of the European Union and the Member States of the European Union.

(6) If, after receipt of the decision, the competent authority of the European Union decides that the amount on the basis of the decision referred to in the second paragraph of this Article is inadmissible, the national supervisory authority shall be bound to this decision and shall, within five days of receipt of this decision, issue the person referred to in the second paragraph Of this Article, a new decision prohibiting the further amount of his personal data.

Recording the amount

Article 71

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

VI. PART
SPECIAL ARRANGEMENTS
Chapter 1
Direct marketing
Rights and duties of the controller
Article 72

(1) The data controller may use the personal data of individuals collected from publicly available sources or in the context of the lawful pursuit of the activity, including for the purpose of offering goods, services, employment or temporary work by using postal services, telephone calls, e-mail Or other telecommunication means (hereinafter referred to as "direct marketing") in accordance with the provisions of this Chapter, unless otherwise provided by another law.

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

(3) The personal data controller shall perform direct marketing in such a way that he informs the individual, when performing direct marketing, of his rights under Article 73 of this Act.

(4) If the personal data controller intends to provide the personal data referred to in the second paragraph of this Article to other users of personal data for the purposes of direct marketing or contracted processors, he shall be obliged to inform the individual thereof and obtain written consent prior to the transmission of his personal data. Notification to the individual about the intended transmission of personal data must contain information on what information he intends to provide, to whom and for what purpose. The cost of the notification is covered by the data controller.

Right of the individual
Article 73

(1) An individual may, at any time, in writing or in any other manner agreed, require the personal data controller to permanently or temporarily discontinue use of his personal data for the purpose of direct marketing. The data controller is obliged within 15 days to adequately prevent the use of

personal data for the purpose of direct marketing, and in the next five days, inform the individual who requested it in writing or otherwise agreed.

(2) The costs of all acts of the data controller in connection with the request referred to in the preceding 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 conduct of video surveillance, unless otherwise provided by law.

(2) A public or private sector video surveillance operator must publish a notice. The notice must be clearly and clearly publicized in such a way as to enable the individual to become acquainted with its implementation at the latest when the video surveillance takes place.

(3) The notice referred to in the preceding paragraph shall contain the following information:

1. to conduct video surveillance;

2. the name of the person of the public or private sector it carries out;

3. phone number to obtain information on where and how long recordings are stored from the video surveillance system.

(4) The notice referred to in the second paragraph of this Article shall be deemed to be informed of the processing of personal data under Article 19 of this Act.

(5) The video surveillance system used for video surveillance must be protected against access by unauthorized persons.

Access to official office or business premises

Article 75

(1) The public and private sector may carry out video surveillance of their access to their official office or business premises, if necessary for the safety of persons or property, in order to ensure the control of entry or exit to or from official or business premises or, due to the nature of the work, Employees. The decision shall be taken by a competent official, head, director or other competent or authorized individual of a public sector entity or a private sector person. In the written decision,

reasons for introducing video surveillance must be justified. The introduction of video surveillance may also be determined by law or by a regulation adopted on its basis.

(2) Video surveillance may only be carried out in such a way that neither the recording of the interior of residential buildings, which has no effect on access to their premises, nor the recording of the entrances to the apartments can be carried out.

(3) The implementation of video surveillance must be notified in writing to all employees in the public or private sector, who work in a controlled area.

(4) The personal data collection referred to in this Article shall contain a record of the individual (picture or voice), the date and time of entry and exit from the premises, as well as the personal name of the recorded individual, the address of his permanent or temporary residence, employment, number and information on his type The identity document and the reason for the entry if such personal data are collected in addition to or with the video surveillance system.

(5) The personal data referred to in the preceding paragraph may be kept for a maximum of one year after the occurrence, and then deleted, unless otherwise provided by the law.

Multi-dwelling buildings

Article 76

(1) The introduction of video surveillance in a multi-apartment building requires the written consent of co-owners, who own more than 70 percent of the co-ownership shares.

(2) Video surveillance may be introduced in a multi-apartment building only when necessary for the safety of people and property.

(3) With video surveillance in a multi-apartment building, only access to the entrances and exits of multi-dwelling buildings and their common spaces can be controlled. It is forbidden to conduct a video surveillance of the housekeeper's apartment and the workshop for the caretaker.

(4) It shall be prohibited to allow or perform on-line or subsequent inspection of the video surveillance system video recordings via an internal cable television, public cable television, the Internet or through another telecommunication means capable of transmitting these recordings.

(5) It is forbidden to record entrances to individual dwellings with a video surveillance system.

Working spaces

Article 77

(1) The implementation of video surveillance within working spaces may be carried out only in exceptional cases where this is indispensable for the security of people or property, or for the protection of classified information and business secrets, and this purpose can not be attained with lenient means.

(2) Video surveillance may only be carried out in relation to those parts of the premises where it is necessary to protect the interests referred to in the preceding paragraph.

(3) Video surveillance in work areas outside the workplace, in particular in changing rooms, elevators and sanitary facilities, is prohibited.

(4) Prior to the commencement of video surveillance, employees must be informed in advance of written notification of its implementation in accordance with this Article.

(5) Prior to the introduction of video surveillance in a public or private sector, the employer must consult a representative trade union with the employer.

(6) In the field of national defense, intelligence and security activities of the State and the protection of classified information, the fourth and fifth paragraphs of this Article shall not apply.

Chapter 3

Biometrics

General provision

Article 78

The processing of biometric features determines or compares the characteristics of an individual so that his identification can be performed or his identity verified (hereinafter: biometric measures) under the conditions laid down in this law.

Biometric measures in the public sector

Article 79

(1) Biometric measures in the public sector may only be determined by law, if this is indispensable for the safety of people or property, or for the protection of classified information and business secrets, and this purpose can not be achieved by lesser means.

(2) Notwithstanding the preceding paragraph, biometric measures may be determined by law in the case of compliance with obligations under a binding international treaty or for identifying individuals when crossing national borders.

Biometric measures in the private sector

Article 80

(1) A private sector may carry out biometric measures only if it is strictly necessary for carrying out activities, for the safety of persons or property, or for the protection of classified information or business secrets. Biometric measures may only be exercised over their employees if they have been informed in writing in advance.

(2) If the implementation of certain biometric measures in the private sector is not regulated by law, the personal data controller intending to carry out biometric measures shall be obliged to submit to the national supervisory authority a description of the intended measures and the reasons for their introduction prior to the imposition of measures.

(3) Upon receipt of the information referred to in the preceding paragraph, the national supervisory authority shall be obliged to decide within two months whether the introduction of biometric measures is intended in accordance with this Act, in particular with the conditions referred to in the first sentence of the first paragraph of this Article. The deadline may be extended by up to one month if the introduction of these measures would affect more than 20 employees in the private sector, or if a representative trade union requests the employer to participate in the administrative procedure.

(4) The personal data controller may perform biometric measures upon receipt of the decision referred to in the preceding paragraph, by which the implementation of biometric measures is permitted.

(5) There shall be no appeal against the decision of the state supervisory authority referred to in the third paragraph of this article, but administrative dispute is allowed.

Biometric measures in relation to public sector employees

Article 81

Notwithstanding the provisions of Article 79 of this Act, biometric measures may be introduced in the public sector in connection with the entry into the building or parts of the building and the recording of the presence of employees at work, which are carried out in the sense of applying the second, third and fourth paragraphs of Article 80 of this Act .

Chapter 4

Record of entries and exits from premises

Evidence

Article 82

(1) A person from the public or private sector may, for the purposes of protecting the property, life or body of individuals and order in its premises from an individual intending to enter or exit the area, indicate all or some of the personal data referred to in the second paragraph of this Article, and The reason for entering or exiting. If necessary, it can also check personal information by looking at the individual's identity document.

(2) In the entry and exit record, only the following personal data may be kept on the individual: the personal name, the number and the type of personal document, the address of permanent or temporary residence, employment and the date, time and the reason for entering or exiting to or from the premises.

(3) The records referred to in the preceding paragraph shall be considered as official records in accordance with the law governing the general administrative procedure, if it is necessary to obtain information from the point of view of the benefit of the minor or for the exercise of police powers and intelligence-security activity.

(4) Personal data from the records referred to in the second paragraph of this Article may be kept for a maximum of three years from the entry, then deleted or otherwise destroyed unless otherwise provided by the law.

Chapter 5

Public books and personal data protection

The legal purpose of the public book

Article 83

Personal data from a public record regulated by law may only be used in accordance with the purpose for which they were collected or processed if the legal purpose of their collection or processing is specified or identifiable.

Chapter 6

Linking personal data collections

Official records and public books

Article 84

(1) Collections of personal data from official records and public books may be combined, if so provided by law.

(2) Operators or controller of personal data that connects two or more personal databases for various purposes shall be obliged to inform the national supervisory authority in writing in advance.

(3) If at least one database of personal data to be linked contains sensitive data, or if the connection would result in the disclosure of sensitive data or the use of the same connecting sign is required to carry out the connection, connection is not allowed without the prior permission of the national supervisory authority Organs.

(4) The national supervisory authority shall authorize the connection referred to in the preceding paragraph on the basis of a written application from the data controller if it finds that the personal data controllers provide adequate personal data protection.

(5) There is no appeal against the decision referred to in the preceding paragraph, but administrative dispute is allowed.

Ban on connection

Article 85

It is forbidden to link collections of personal data from criminal records and misdemeanor records to other collections of personal data and to link collections of personal data from criminal records and misdemeanor records.

Special provision

Article 86

In the database of personal data collections, data on related personal data collections from official records and public books are kept separately.

Chapter 7

Professional supervision

Application of the provisions of this chapter

Article 87

Unless otherwise provided by another law, the provisions of this Chapter shall apply to the processing of personal data for the purposes of professional supervision, as laid down by law.

General provisions

Article 88

(1) A public sector entity carrying out expert supervision (hereinafter referred to as the expert control expert) may process personal data processed by personal data controllers, over which it has the competence to exercise expert supervision under the law.

(2) The professional controller shall have the right to inspect, print out, copy or copy all personal data referred to in the preceding paragraph, and in the course of their processing for the purposes of professional supervision and the preparation of a report or assessment, he shall be obliged to protect their confidentiality. In a report or an assessment at the end of professional supervision, the professional supervisor may record only those personal data that are necessary to achieve the purpose of professional supervision.

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

Professional supervision and additional processing of personal data

Article 89

(1) When carrying out expert supervision in which he processes personal data in accordance with the first paragraph of Article 88 of this Act, the professional supervision expert may inform the data subject in writing in writing to the professional data and inform him that he can write in writing Or make oral submissions.

(2) The individual referred to in the preceding paragraph may submit to the provider of professional supervision for the purpose of carrying out expert supervision the personal data of another individual who could know about the matter in which the expert supervision is carried out. If the professional supervisor finds that this is necessary, he / she shall also conduct an interview with another individual.

Professional supervision and sensitive personal data

Article 90

If sensitive information is processed in the exercise of professional supervision, the professional controller makes an official endorsement or other official record in the case file of the data controller.

VII. PART

PENALTY PROVISIONS

General breaches of the provisions of this Act

Article 91

(1) A fine of 4,170 to 12,510 euros shall be imposed on a legal person, an individual sole proprietor or an individual who performs an activity independently:

1. if he processes personal data without having such a basis in the law or in the personal consent of the individual (Article 8);

2. if he entrusts certain tasks with regard to the processing of personal data to another person without concluding a contract in accordance with Article 11, paragraph 2;

3. if he processes sensitive personal data in violation of Article 13 or does not insure them in accordance with Article 14;

4. automated processing of personal data in contravention of Article 15;

5. if it collects personal data for purposes other than specified and lawful, or if it processes them further in violation of Article 16;

6. if he transmits personal data to the user of personal data in contravention of the second paragraph of Article 17 or if he does not destroy personal data in accordance with paragraph 3 of Article 17 or does not publish the results of processing in accordance with Article 17, paragraph 4;

7. failing to inform an individual of the processing of personal data in accordance with Article 19;

8. if he uses the same connecting sign in contravention of Article 20;

9. if it does not delete, destroy, block or anonymize personal data after the purpose of processing has been completed in accordance with Article 21, paragraph 2;

10. if he acts contrary to article 22;

11. failing to ensure that the catalog of the personal data database contains the information provided by the law (Article 26);

12. failing to provide data for the needs of the database of personal data collections (Article 27);

13. if he acts contrary to the first or second paragraph of Article 30 or if he acts in contravention of the second, third or fifth paragraph of Article 31;

14. if he acts contrary to Article 32 or if he acts contrary to the second or fifth paragraph of Article 33;

15. if, contrary to the first paragraph of Article 63 or, contrary to Article 70, he transfers personal data to a third country.

(2) The offense referred to in the preceding paragraph shall also be imposed on the responsible person of a legal person, sole proprietor of an individual or an individual who performs an activity independently from a fine of 830 to 2,080 euros.

(3) The responsible person of a state body or a body of a self-governing local community who commits an act referred to in the first paragraph of this Article shall be fined for a misdemeanor from 830 to 2 080 euros.

(4) A fine of 200 to 830 euros shall be imposed on an individual who commits an act referred to in the first paragraph of this Article for an offense.

Breach of the provisions on contractual processing

Article 92

(1) A fine of 4,170 to 12,510 euros shall be imposed on a legal person, an individual sole proprietor or an individual who performs an activity independently if he exceeds the powers contained in the contract referred to in the second paragraph of Article 11 or does not return his personal data in accordance with the third Paragraph 11 of Article 11.

(2) The offense referred to in the preceding paragraph shall also be imposed on the responsible person of a legal person, sole proprietor of an individual or an individual who performs an activity independently from a fine of 830 to 2,080 euros.

(3) The responsible person of a state body or a body of a self-governing local community who commits an act referred to in the first paragraph of this Article shall be fined for a misdemeanor from 830 to 2 080 euros.

(4) A fine of 200 to 830 euros shall be imposed on an individual who commits an act referred to in the first paragraph of this Article for an offense.

Breach of the provisions on the protection of personal data

Article 93

(1) A fine of 4,170 to 12,510 euros shall be imposed on a legal person, a sole proprietor or an individual who performs an activity independently, if he processes personal data in accordance with this Act and does not provide personal data protection (Articles 24 and 25).

(2) The offense referred to in the preceding paragraph shall also be imposed on the responsible person of a legal person, sole trader of an individual or an individual who performs an activity independently from a fine of EUR 830 to EUR 1,250.

(3) A fine of 830 to 1,250 euros shall be imposed on a responsible person of a state authority or authority of a self-governing local community for an offense committing an act referred to in the first paragraph of this Article.

(4) A fine of 200 to 830 euros shall be imposed on an individual who commits an act referred to in the first paragraph of this Article for an offense.

Breach of provisions on direct marketing

Article 94

(1) A fine of EUR 2,080 to EUR 4,170 shall be imposed on a legal person, an individual sole proprietor or an individual who performs an activity independently, if he processes personal data for the purposes of direct marketing in accordance with this Act and does not comply with the 72nd or Article 73.

(2) A fine of between 410 and 1,250 euros shall also be imposed on the responsible person of a legal person, sole proprietor of an individual or an individual who performs an activity independently for the offense referred to in the preceding paragraph.

(3) A fine of 200 to 830 euros shall be imposed on an individual who commits the act referred to in the first paragraph of this Article for an offense.

Violation of general video surveillance provisions

Article 95

(1) A fine of 4,170 to 12,510 euros shall be imposed on a legal person, an individual sole proprietor or an individual who performs an activity independently:

1. if he does not publish the notice in the manner referred to in the second paragraph of Article 74;

2. if the notice does not contain the information referred to in the third paragraph of Article 74;

3. if it does not insure the video surveillance system with which the video surveillance is carried out, contrary to the fifth paragraph of Article 74.

(2) The offense referred to in the preceding paragraph shall also be imposed on the responsible person of a legal person, sole trader of an individual or an individual who performs an activity independently from a fine of EUR 830 to EUR 1,250.

(3) A fine of 830 to 1,250 euros shall be imposed on a responsible person of a state authority or authority of a self-governing local community for an offense committing an act referred to in the first paragraph of this Article.

(4) A fine of 200 to 830 euros shall be imposed on an individual who commits the act referred to in the first paragraph of this Article for an offense.

Violation of video surveillance provisions regarding access to official office or business premises

Article 96

(1) A fine of 4,170 to 12,510 euros shall be imposed on a legal person, an individual sole proprietor or an individual who performs an activity independently:

1. he / she executes a video surveillance service without a reasoned written decision or no other legal basis from the first paragraph of Article 75;

2. executes the video surveillance by recording the interior of residential buildings which do not affect the access to their premises or the recording of the entrance to the apartments (second paragraph of Article 75);

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

4. if it stores personal data contrary to Article 75 (5).

(2) The offense referred to in the preceding paragraph shall also be imposed on the responsible person of a legal person, sole trader of an individual or an individual who performs an activity independently from a fine of EUR 830 to EUR 1,250.

(3) A fine of 830 to 1,250 euros shall be imposed on a responsible person of a state authority or authority of a self-governing local community for an offense committing an act referred to in the first paragraph of this Article.

(4) A fine of 200 to 830 euros shall be imposed on an individual who commits the act referred to in the first paragraph of this Article for an offense.

Violation of video surveillance provisions for multi-dwelling buildings

Article 97

(1) A fine of EUR 2,080 to EUR 8,340 shall be imposed on a legal person, an individual sole proprietor or an individual who independently carries out a video surveillance activity in violation of Article 76.

(2) A fine of between 410 and 1,250 euros shall also be imposed on the responsible person of a legal person, sole proprietor of an individual or an individual who performs an activity independently for the offense referred to in the preceding paragraph.

(3) A fine of 830 to 1,250 euros shall be imposed on a responsible person of a state authority or authority of a self-governing local community for an offense committing an act referred to in the first paragraph of this Article.

(4) A fine of 200 to 410 euros shall be imposed on an individual who commits an act referred to in the first paragraph of this Article for an offense.

Violation of video surveillance provisions in work areas

Article 98

(1) A fine of EUR 4,170 to EUR 12,510 shall be imposed on a legal person, an individual sole proprietor or an individual who performs an activity that performs a surveillance of the workplace in contravention of Article 77.

(2) A fine of EUR 1,250 to 2,080 shall also be imposed on a responsible person of a legal person, sole proprietor of an individual or an individual who performs an activity independently of the offense referred to in the preceding paragraph.

(3) A fine of 1,250 to 2,080 euros shall be imposed on a responsible person of a state authority or authority of a self-governing local community for an offense committing an act referred to in the first paragraph of this Article.

(4) A fine of EUR 830 to 1,200 shall be imposed on an individual who commits an act referred to in the first paragraph of this Article for an offense.

Violation of the provisions on public sector biometrics

Article 99

(1) A fine of 4,170 to 12,510 euros shall be imposed on a public sector legal entity responsible for biometric measures in violation of Article 79.

(2) A fine of EUR 1,250 to 2,080 shall also be imposed on the responsible person of the public sector legal entity for the offense referred to in the preceding paragraph.

(3) A fine of 1,250 to 2,080 euros shall also be imposed on the responsible person of a state authority or authority of a self-governing local community for the offense referred to in the first paragraph of this Article which commits an act referred to in the first paragraph of this Article.

Breach of the provisions on biometrics in the private sector

Article 100

(1) A fine of 4,170 to 12,510 euros shall be imposed on a legal person, an individual sole proprietor or an individual who performs an activity that performs biometric measures in violation of Article 80.

(2) A fine of EUR 1,250 to 2,080 shall also be imposed on a responsible person of a legal person, sole proprietor of an individual or an individual who performs an activity independently of the offense referred to in the preceding paragraph.

Violation of the provisions on entry and exit records

Article 101

(1) A fine of 2,080 to 4,170 euros shall be imposed on a legal person, an individual sole trader or an individual performing an activity independently:

1. who uses the entry and exit records as an official record in violation of Article 82 (3);

2. who acts contrary to the fourth paragraph of Article 82.

(2) A fine of between EUR 200 and EUR 830 shall also be imposed on a responsible person of a legal person, sole proprietor of an individual or an individual who independently performs an activity that commits an offense referred to in the preceding paragraph.

(3) A fine of 200 to 830 euros shall be imposed on a responsible person of a state authority or authority of a self-governing local community for an offense referred to in the first paragraph of this article.

(4) A fine of 200 to 410 euros shall be imposed on an individual who commits an offense referred to in the first paragraph of this Article for an offense.

Violation of the provisions on the linking of personal data collections

Article 102

(1) A fine of 830 to 2 080 euros shall be imposed on a responsible person of a state authority or self-governing local community for the violation of the collection of personal data contrary to the third paragraph of Article 84.

(2) A fine of EUR 830 to 2 080 shall be imposed on a responsible person of a state authority or self-governing local community who links collections of personal data from criminal records and misdemeanor records to other collections of personal data or links collections of personal data from a criminal record with a collection of personal data Data from misdemeanor records (Article 85).

Breach of professional supervision provisions

Article 103

(1) A fine of 4,170 to 12,510 euros shall be imposed on a legal person for the offense:

1. if he exercises professional supervision contrary to the second paragraph of Article 88;

2. failing to make an official endorsement or other official record in contravention of Article 90 of this Act.

(2) A fine of EUR 830 to EUR 1,250 shall also be imposed on the responsible person of a legal person for the offense referred to in the preceding paragraph.

(3) A fine of 830 to 1,250 euros shall be imposed on a responsible person of a state authority or authority of a self-governing local community for an offense committing an act referred to in the first paragraph of this Article.

(4) A fine of 200 to 830 euros shall be imposed on an individual who commits an act referred to in the first paragraph of this Article for an offense.

The Personal Data Protection Act - ZVOP-1 (Official Gazette of the Republic of Slovenia, No. 86/04) contains the following transitional and final provisions:

VIII. PART

TRANSITIONAL AND FINAL PROVISIONS

Responsibilities of the Commissioner for access to information of a public nature with regard to the protection of personal data

Article 104

- considered ZInfP

(Expired)

Deadline for issuing implementing regulations

Article 105

(1) The rules referred to in 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 referred to in the second paragraph of Article 52 of this Act shall be issued by 1 January 2006.

Transitional arrangements

Article 106

(1) Public funds may be processed and collected on the basis of personal consent from individuals of personal data relating to them, provided that such information is necessary and appropriate for the performance of their duties and competences, irrespective of the provisions of the laws governing their tasks and competences And the provisions of this Act, pending the entry into force of a special law regulating these issues.

(2) The data controllers may communicate to the public and publicly disclose their personal name, title or function, the official telephone number and the address of the official e-mail of the head and those employees whose work is important for dealing with customers or users of services until the entry into force of a special law He will handle these questions.

Expression of the data controller

Article 107

The terms "database manager", "data controller" or "database manager" or "database manager" specified in the laws are deemed to be the term "data controller" under this Act.

Establishment of the National Supervisory Authority for the Protection of Personal Data

Article 108

- considered ZInfP

(Expired)

Appointment of the Chief State Supervisor

Article 109

- considered ZInfP

(Expired)

Recruitment of employees and archives

Article 110

- considered ZInfP

(Expired)

Application of individual provisions of this Act

Article 111

(1) The provisions of the second paragraph of Article 48 and points 3 and 4 of the first paragraph of Article 49 of this Act shall apply from the day of the commencement of the activities of the National Supervisory Body for the Protection of Personal Data.

(2) Pending the establishment of the website of the National Supervisory Body for the Protection of Personal Data, information published under the Act by the State Supervisory Body on its website shall be published on the website of the Ministry of Justice.

Complete the running procedures

Article 112

If the decision or decision of the inspector is issued before the entry into force of this Act, the procedure shall end according to the provisions of the Personal Data Protection Act (Official Gazette RS, No. 59/99, 57/01, 59/01 - p. 52/02 - ZDU- 1 and 73/04 - ZUP-C).

Transfer of keeping the register of personal data collections

Article 113

(1) A common catalog of personal data, which is conducted in accordance with the provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99,

57/01, 59/01 - p. 52/02 - ZDU-1 and 73 / 04 - ZUP-C), shall be renamed as a register of personal data collections from the date of entry into force of this Act.

(2) Until 1 January 2006, the Ministry of Justice shall keep and maintain the register referred to in the preceding paragraph, and on this date it shall submit it to the National Supervisory Body for the Protection of Personal Data.

Updating the data in the database of personal data collections

Article 114

Managers of personal data who provided personal data in accordance with the provisions of the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01 - p. 52/02 - ZDU-1 and 73/04 - ZUP-C) must submit to the competent body referred to in Article 113 of this Act all data referred to in Article 27 of this Act within one year after the entry into force of the implementing regulation referred to in the third paragraph of Article 28 of this Act.

Termination

Article 115

(1) On the day this Act enters into force, the Personal Data Protection Act (Official Gazette of the Republic of Slovenia, No. 59/99, 57/01, 59/01 - pg., 52/02 - ZDU-1 and 73/04 - ZUP -C).

(2) On the day of the commencement of the work of the National Supervisory Body for the Protection of Personal Data, the second indent of the first paragraph and the third paragraph of Article 13 of the Decree on bodies within the composition of ministries (Official Gazette of the Republic of Slovenia, No. 58/03) shall cease to apply.

(3) As of the date of entry into force of this Act, 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 apply in so far as they determine the collection, processing and publication of the EMŠO - Citizen identification number.

Change in another law

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 text "science and technology" is replaced by "justice «.

Entry into force

Article 117

This Act shall enter into force on 1 January 2005.

The Act Amending and Supplementing the Personal Data Protection Act - ZVOP-1A (Official Gazette of the Republic of Slovenia, No. 67/07) contains the following transitional and final provision:

Transitional provision

Article 17

The minister responsible for justice shall issue the rules referred to in the seventh paragraph of Article 31 of the law within sixty days after the entry into force of this Act.

Final provision

Article 18

This Act shall enter into force on the day following its publication in the Official Gazette of the Republic of Slovenia, and Article 3 of this Act shall apply on the sixtieth day after the publication of this Act.

https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina?urlurid=20074690