Act Amending the Personal Data Protection Act (ZVOP-1A)

Date of adoption	12.07.2007	EVA	2007-2011-0070
Date of publication	27.07.2007	EPA	1462-IV
Date of entry into force	28.07.2007	SOP	2007-01-3701

Link to the Official Journal:
Official Gazette of the RS, no. 67/07

Unofficial consolidated text containing this change:

Note: The unofficial consolidated text of the regulation is only an informative work tool, for which the body does not guarantee compensation or otherwise.

The unofficial consolidated text of the Personal Data Protection Act includes:
- Personal Data Protection Act - ZVOP-1 (Official Gazette of the Republic of Slovenia, No. 86/04 of 5 August 2004),
- Information Commissioner Act - ZInfP (Official Gazette of the Republic of Slovenia, No. 113/05 of 16 December 2005),
- Act Amending the Constitutional Court Act - ZUstS-A (Official Gazette of the Republic of Slovenia, No. 51/07 of 8 June 2007),
- Act Amending the Personal Data Protection Act - ZVOP-1A (Official Gazette of the Republic of Slovenia, No. 67/07 of 27 July 2007).

L A W
ON THE PROTECTION OF PERSONAL DATA (ZVOP-1)

(Unofficial consolidated text No 3)

PART I
GENERAL PROVISIONS

Content of the law

Article 1

This Act determines the rights, obligations, principles and measures that prevent unconstitutional, illegal and unjustified encroachments on the privacy and dignity of the individual (hereinafter: the individual) in the processing of personal data.

The principle of legality and fairness

Article 2

Personal data is processed lawfully and fairly.

Proportionality principle

Article 3

The personal data being processed must be relevant and appropriate in scope to the purposes for which they are collected and further processed.

Prohibition of discrimination

Article 4

The protection of personal data is guaranteed to every individual, regardless of nationality, race, color, religion, ethnicity, sex, language, political or other beliefs, sexual orientation, financial status, birth, education, social status, citizenship, place or type of residence or any other personal circumstance.

Territorial application of this Act

Article 5

(1) This Act applies to the processing of personal data if the personal data controller is established, established 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 personal data controller is not established, has no registered office or is not registered in a Member State of the European Union or is not part of the European Economic Area and uses automatic or other equipment located in the Republic of Slovenia. if this equipment is used only for the transfer of personal data through the territory of the Republic of Slovenia.

(3) The personal data controller referred to in the preceding paragraph must designate a natural or legal person who has its registered office or is registered in the Republic of Slovenia and represents him or her regarding the processing of personal data in accordance with this Act.

(4) This Act also applies to diplomatic and consular and other official missions of the Republic of Slovenia abroad.

The meaning of terms

Article 6

The terms used in this Act have the following meanings:

1. Personal data - is any data relating to an individual, regardless of the form in which it is expressed.
2. Individual - is an identifiable or identifiable natural person to whom personal data relates; a natural person is identifiable if he or she can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity. causes high costs, disproportionate effort or does not require much time.
3. Processing of personal data - means any operation or series of operations carried out in relation to personal data which are automatically processed or which are part of a personal data file or intended for inclusion in a personal data file, in particular collection, retrieval, subscribing, editing, storing, adapting or modifying, retrieving, viewing, using, disclosing, communicating, disseminating or otherwise making available, classifying or linking, blocking,

anonymising, deleting or destroying; processing can be manual or automated (processing means).

4. Automated processing - is the processing of personal data by means of information technology.
5. Personal data file - is any structured set of data 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 into 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 identifiability of an individual.
6. Personal data controller - is a natural or legal person or other person of the public or private sector who alone or together with others determines the purposes and means of personal data processing or a person determined by law who also determines the purposes and means of processing.
7. Contractual processor - is a natural or legal person who processes personal data in the name and on behalf of the personal data controller.
8. User of personal data - is a natural or legal person or other person of the public or private sector to whom personal data is transferred or disclosed.
9. Transmission of personal data - is the transmission or disclosure of personal data.
10. Foreign user and foreign controller of personal data - is a user of personal data in a third country and a controller of personal data in a third country.
11. Third country - is a country that is not a Member State of the European Union or part of the European Economic Area.
12. Catalog of the personal data collection - is a description of the personal data collection.
13. Register of personal data files - is a register containing data from catalogs of personal data files.
14. Personal consent of an individual - is a voluntary statement of the will of an individual that his personal data may be processed for a specific purpose, and is given on the basis of information to be provided by the controller under this Act; the personal consent of the individual may be the written, oral or other appropriate consent of the individual.
15. Written consent of the individual - is the signed consent of the individual, which has the form of a document, provisions in the contract, provisions in the contract, annexes to the application or other form in accordance with the law; a signature is also, on the basis of a law, a uniform form given by telecommunication, and on the basis of a law signed a uniform form given by an individual who cannot or cannot write.
16. Oral or other appropriate consent of an individual - is oral or by telecommunication or other appropriate means or in another appropriate manner given consent from which it is possible to unambiguously infer the consent of the individual.
17. Blocking - is the marking of personal data in such a way as to limit or prevent their further processing.
18. Anonymisation - is such a change in the form of personal data that it can no longer be linked to the individual or only with disproportionate effort, cost or time.
19. Sensitive personal data - are data on racial, ethnic or ethnic origin, political, religious or philosophical beliefs, trade union membership, health status, sexual life, entry or deletion 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 makes it possible to identify an individual in relation to any of the above circumstances.
20. The same connecting marks - are personal identification numbers and other unique identification numbers of an individual defined by law, using which it is possible to collect or retrieve personal data from those personal data collections in which the same connecting marks are also processed.
21. Biometric characteristics - are such physical, physiological and behavioral characteristics that all individuals have, but are unique and permanent for each individual and it is possible to determine the individual, especially using a fingerprint, image of papillary lines from the finger, iris , retina, face, ears, deoxyribonucleic acid and characteristic posture.

22. Public sector - are state bodies, bodies of self-governing local communities, holders of public authority, public agencies, public funds, public institutes, universities, independent higher education institutions and self-governing national communities.
23. Private sector - are legal and natural persons performing an activity under the law governing companies or public utility services or crafts, and persons of private law; the private sector is public economic institutes, public companies and companies, regardless 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 carried out by individuals exclusively for personal use, family life or for other domestic needs.

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

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

(4) Personal data controllers with less than 50 employees need not 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 files maintained by personal data controllers from the public sector, notaries, lawyers, detectives, bailiffs, private security providers, private healthcare professionals, healthcare providers and personal data controllers, who maintain databases containing sensitive personal data and the processing of sensitive personal data is part of their registered activity.

II. PART
PROCESSING OF PERSONAL DATA

Chapter 1
Legal bases and purposes

General definition

Article 8

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

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

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 the personal data being processed is determined by law. The law may stipulate that certain personal data may be processed only with the personal consent of the individual.

(2) Holders of public authorizations may also process personal data on the basis of the personal consent of an individual without a basis in law, when it is not a question of performing their tasks as holders of public authorizations. The databases of personal data created on this basis must be separated from the databases of personal data created on the basis of the performance of the tasks of the holder of public authority.

(3) Notwithstanding the first paragraph of this Article, personal data of individuals who have concluded a contract with the public sector or are on the basis of an individual's initiative in the negotiation phase may be processed in the public sector if personal data processing is necessary and suitable for negotiating or concluding a contract.

(4) Notwithstanding the first paragraph of this Article, personal data that are necessary for the exercise of lawful powers, tasks or obligations of the public sector may exceptionally be processed in the public sector, provided that such processing does not interfere with the legitimate interests of the data subject. 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 being processed is determined by law or if the personal consent of the individual is given for the processing of certain personal data.

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

(3) Notwithstanding the first paragraph of this Article, personal data may be processed in the private sector if this is necessary for the realization of 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 related to the processing of personal data with a contract to a contractual processor who is registered to perform such activity and provides appropriate procedures and measures referred to in Article 24 of this Act.

(2) The contractual processor may perform individual tasks related to the processing of personal data within the scope of the client's authorizations and may not process personal

data for any other purpose. Mutual rights and obligations shall be regulated by a contract, which must be concluded in writing and must also contain an agreement on the procedures and measures referred to in Article 24 of this Act. The personal data controller 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 personal data controller and the contractual processor, the contractual processor shall, at the request of the controller, return the personal data which he has contractually processed to the controller. Any copies of this information must be destroyed immediately or forwarded to the state authority competent in accordance with the law to detect or prosecute criminal offenses, to a court or other state authority, if so provided by law.

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

Protecting the vital interests of the individual

Article 12

If the processing of personal data is strictly necessary to protect the life or body of an individual, his or her personal data may be processed, notwithstanding the fact that there is no other legal basis for the processing of such data.

Processing of sensitive personal data

Article 13

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

1. if the individual has given explicit personal consent, which is usually in writing, but also determined by law in the public sector;
2. if the processing is necessary for the fulfillment of obligations and special rights of the personal data controller in the field of employment in accordance with the law, which also determines the appropriate guarantees of the rights of the individual;
3. if the processing is strictly necessary to protect the life or body of the data subject or other persons, when the data subject is physically or commercially unable to give his or her consent referred to in point 1 of this Article;
4. if they are processed for the purposes of lawful activities by institutions, associations, societies, religious communities, trade unions or other non-profit organizations for political, philosophical, religious or trade union purposes, but only if the processing relates to their members or individuals they shall be in regular contact with them in relation to these objectives, and if this information is not passed on to other individuals or persons in the public or private sector without the written consent of the data subject;
5. if the data subject has made it public without the express or explicit intention of limiting the purpose for which it is used;
6. if they are processed by health professionals and health care associates in accordance with the law for the purposes of health care for the population and individuals and for the management or provision of health services;
7. if this is necessary for the purpose of asserting or opposing a legal claim;
8. if so provided by another law for the purpose of exercising the public interest.

Securing sensitive personal data

Article 14

(1) Sensitive personal data must be specially marked and protected during processing in such a way as to prevent unauthorized persons from accessing them, except in the case referred to in point 5 of Article 13 of this Act.

(2) When transmitting sensitive personal data over telecommunication networks, the data shall be deemed to be adequately protected if they are transmitted using cryptographic methods and electronic signature in such a way as to ensure their illegibility or unrecognizability during transmission.

Automated decision making

Article 15

Automated processing of personal data, where a decision may be taken on an individual which has or has a significant effect on him or her and which is based solely on automated data processing designed to evaluate certain personal aspects relating to him or her, such as, in particular, his performance, creditworthiness, reliability, conduct or compliance with the required conditions, is only permitted if the decision is:

1. taken during the conclusion or performance of the contract, provided that the initiative to conclude or perform the contract submitted by the data subject is fulfilled or that appropriate measures are in place to protect his or her legitimate interests, such as , which enable him to object to such a decision or to express his views;
2. determined by law, which also determines measures for the protection of the legitimate interests of the data subject, in particular the possibility of a legal remedy against such a decision.

Purpose of collection and further processing

Article 16

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

Processing for historical, statistical and scientific research purposes

Article 17

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

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

(3) Personal data that have been transmitted to the user of personal data in accordance with the preceding paragraph shall be destroyed upon completion of processing, unless otherwise provided by law. The user of personal data must inform the personal data

controller to whom the personal data were transferred in writing without delay after their destruction, when and in what way he destroyed them.

(4) The results of the processing referred to in the first paragraph of this Article shall be published in anonymised form, unless otherwise provided by law or if the data subject has given written consent for publication in non-anonymised form or if written consent has been given. heirs of the deceased under this Act.

Chapter 2
Protection of individuals

Accuracy and up-to-dateness of personal data

Article 18

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

(2) Before entering into the personal data file, the personal data controller may verify the accuracy of personal data by inspecting the personal document or other relevant public document of the individual to whom they relate.

Informing the individual about the processing of personal data

Article 19

(1) If personal data are collected directly from the data subject, the personal data controller or his representative must communicate the following information to the individual if the individual is not already aware of them:
- data on the personal data controller and his / her potential representative (personal name, title or company name and address or registered office),
- the purpose of the processing of personal data.

(2) If, given the special circumstances of personal data collection referred to in the previous paragraph, it is necessary to ensure lawful and fair processing of personal data, the person referred to in the previous paragraph must also provide additional information to the individual if the individual is not yet familiar with them.
- an indication of the user or type of user of his personal data,
- an indication of whether the collection of personal data is mandatory or voluntary, and the possible consequences of not providing data voluntarily,
- information on the right to inspect, transcribe, copy, supplement, correct, block and delete personal data relating to him.

(3) If personal data have not been collected directly from the data subject, the personal data controller or his representative must communicate the following information to the data subject at the latest when entering or transmitting personal data:
- data on the personal data controller and his / her potential representative (personal name, title or company name and address or registered office),
- the purpose of the processing of personal data.

(4) If, in view of the special circumstances of the collection of personal data referred to in the preceding paragraph, it is necessary to ensure lawful and fair processing of personal data,

the person referred to in the preceding paragraph must also communicate additional information to the individual, in particular:
- information on the type of personal data collected,
- an indication of the user or type of user of his personal data,
- information on the right to inspect, transcribe, copy, supplement, correct, block and delete personal data relating to him.

(5) The information referred to in the third and fourth paragraphs of this Article need not be provided if this would be impossible due to the processing of personal data for historical, statistical or scientific research purposes or would cause high costs, disproportionate effort or time or if the law explicitly provides for the entry or transmission of personal data.

Using the same hyphen

Article 20

(1) When obtaining personal data from personal data files in the field of health, police, intelligence and security activities of the state, defense of the state, judiciary and public prosecutor's office, as well as criminal records and misdemeanor records, the use of the same connecting sign may not be used. personal data used only this sign.

(2) Notwithstanding the preceding paragraph, the same connecting sign may exceptionally be used for the acquisition of personal data if this is the only data in a specific case that can enable the detection or prosecution of a criminal offense ex officio to protect life or body individual or to ensure the performance of the tasks of the intelligence and security authorities established by law. An official note 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.

Term of retention of personal data

Article 21

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

(2) After fulfilling the purpose of processing, personal data shall be deleted, destroyed, blocked or anonymised if they are not defined as archives on the basis of the law governing archives and archives, or unless otherwise provided by law for individual types of personal data.

Transmission of personal data

Article 22

(1) The controller of personal data must provide personal data to users of personal data against the payment of costs of transmission, unless otherwise provided by law.

(2) The administrator of the central population register or records of permanently and temporarily registered residents must provide the beneficiary who has a legal interest in

exercising rights before public sector persons with the personal name and address of permanent or temporary residence of the individual, against which he exercises his rights.

(3) For each transfer of personal data, the personal data controller must ensure that it is possible to determine later which personal data were transferred, to whom, when and on what basis, for the period when legal protection of the individual's rights due to inadmissible transfer is possible. personal data.

(4) Notwithstanding the first paragraph of this Article, the controller of personal data in the public sector is obliged to provide personal data to the user of personal data in the public sector without payment of transmission costs, unless otherwise provided by law or for historical, statistical or scientific research. purpose.

Protection of personal data of deceased individuals

Article 23

(1) The personal data controller may provide data on a deceased individual only to those users of personal data who are authorized by law to process personal data.

(2) Notwithstanding the previous paragraph, the personal data controller shall forward data on the deceased individual to the person who, according to the law governing inheritance, is his legal heir of the first or second hereditary order, if he shows a legal interest in using personal data. prohibit the transmission of this personal data.

(3) Unless otherwise provided by law, the personal data controller may also transfer the data referred to in the preceding paragraph to any other person who intends to use such data for historical, statistical or scientific research purposes, unless the deceased has prohibited the transmission of such personal data.

(4) If the deceased individual has not submitted the prohibition referred to in the preceding paragraph, persons who are his legal heirs of the first or second hereditary order according to the law governing inheritance may prohibit the transmission of his data in writing, unless otherwise provided by law.

Chapter 3
Protection of personal data

Content

Article 24

(1) The protection of personal data comprises organizational, technical and logical-technical procedures and measures by which personal data are protected, prevents accidental or intentional unauthorized destruction of data, alteration or loss and unauthorized processing of such data by:

1. protect premises, equipment and system software, including input-output units;
2. protects the application software with which personal data are processed;
3. prevent unauthorized access to personal data during their transfer, including transmission via telecommunications and networks;
4. provides an effective means of blocking, destroying, deleting or anonymising personal data;

5. enables later determination of when individual personal data were entered into the personal data file, used or otherwise processed and who did so, for the period when legal protection of the individual's rights due to inadmissible transmission or processing of personal data is possible.

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

(3) Procedures and measures for the protection of personal data must be appropriate in view of the risk posed by the processing and the nature of certain personal data being processed.

(4) Officials, employees and other individuals who perform work or tasks for persons who process personal data shall be obliged to protect the confidentiality of personal data with which they become acquainted in the performance of their functions, works and tasks. The duty to protect the confidentiality of personal data also binds them after the termination of their function, employment, performance of work or tasks or provision of contractual processing services.

Duty of insurance

Article 25

(1) Personal data controllers and contractual processors are obliged to ensure the protection of personal data in the manner referred to in Article 24 of this Act.

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

Chapter 4
Information on personal data files

Catalog of personal data collection

Article 26

(1) For each personal data file, the personal data controller shall establish a catalog of the personal data file, which shall contain:
1. name of the personal data file;
2. data on the personal data controller (for a natural person: personal name, address of activity or address of permanent or temporary residence, for a sole proprietor of an individual also the company name, registered office and registration number; for a legal entity: name or company name and address or registered office of the controller personal data and registration number);
3. the legal basis for the processing of personal data;
4. the categories of data subjects;
5. types of personal data in the personal data file;
6. purpose of processing;
7. period of retention of personal data;

8. restrictions on the rights of individuals with regard to personal data in the personal data file and the legal basis for the restrictions;
9. users or categories of users of personal data contained in the personal data file;
10. the fact that personal data are transferred to a third country, where, to whom and the legal basis of the export;
11. general description of personal data protection;
12. data on related personal data collections from official records and public books;
13. data 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 an individual sole proprietor the company name, registered office and registration number; for legal person: title or company name and address or registered office of the personal data controller and registration number).

(2) The controller of personal data must take care of the accuracy and timeliness of the content of the catalog.

Informing the supervisory authority

Article 27

(1) The personal data controller shall forward the data referred to in items 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 protection of personal data at least 15 days before the establishment of the personal data file or before the entry of a new type of personal data.

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

(3) **(deletion)** .

Register

Article 28

(1) The State Supervisory Body for the Protection of Personal Data shall keep and maintain a register of personal data files containing the data referred to in Article 27 of this Act in the manner determined by the methodology of its management.

(2) The register shall be kept by means of information technology and shall be 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 responsible for justice on the proposal of the Chief State Supervisor or the Chief State Supervisor for Personal Data Protection (hereinafter: the Chief State Supervisor).

III. PART
OF THE RIGHT OF THE INDIVIDUAL

Insight into the register

Article 29

(1) The state supervisory body for the protection of personal data must allow everyone access to the register of personal data files and a transcript of data.

(2) Access to and transcription of data must be permitted and made possible, as a rule, on the same day, but no later than within eight days, otherwise the request shall be deemed to have been rejected.

The right of the individual to be informed

Article 30

(1) The controller of personal data must, at the request of an individual:

1. provide access to the catalog of the personal data file;
2. confirm whether or not the data related to him are processed and enable him to inspect and transcribe or copy the personal data contained in the personal data file and relating to it;
3. provide a printout of personal data contained in the personal data file and relating to it;
4. provide a list of users to whom personal data have been provided, when, on what basis and for what purpose;
5. provide information on the sources on which the records contained in the personal data file are based and on the method of processing;
6. provide information on the purpose of the processing and the type of personal data being processed, as well as any necessary explanations in this regard;
7. explain technical or logical-technical decision-making procedures if he / she performs automated decision-making by processing personal data of an individual.

(2) The extract referred to in point 3 of the preceding paragraph may not replace a document or certificate in accordance with the regulations on administrative or other procedures, which shall be indicated on the extract.

Pairing process

Article 31

(1) The request referred to in Article 30 of this Act shall be submitted in writing or orally to the minutes with the personal data controller. The request may be made once every three months, regarding the processing of sensitive personal data and personal data in accordance with the provisions of Chapter 2 of VI. part of this law once a month. Where necessary to ensure the fair, lawful or proportionate processing of personal data, in particular where the personal data of an individual in the personal data file are frequently updated or provided or could be frequently updated or provided to users of personal data, the controller should allow the individual to request also within a shorter relevant period, which is not less than five days from the day of acquaintance with personal data relating to him or refusal of such acquaintance.

(2) The personal data controller must enable the individual to inspect, transcribe, copy and confirm under items 1 and 2 of the first paragraph of Article 30 of this Act, as a rule on the same day as the request, but within 15 days or within 15 days. days in writing of the reasons why it will not allow inspection, transcription, copying or issuance of the certificate.

(3) The statement referred to in point 3, the list referred to in point 4, the information referred to in points 5 and 6 and the explanation referred to in point 7 of the first paragraph of Article 30 of this Act must be provided to the individual within 30 days. received a request to inform him in writing within the same time limit of the reasons why he will not provide him with a printout, list, information or explanation.

(4) If the administrator does not act in accordance with the second and third paragraphs of this Article, the request shall be deemed to have been rejected.

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

(6) For transcripts, copies and written confirmations under point 2 and for the extract referred to in point 3, the list referred to in point 4, the information referred to in points 5 and 6 and the explanation referred to in point 7 of the first paragraph of Article 30 of this Act the controller of personal data charges the individual only material costs according to a predetermined price list, with oral confirmation according to point 2, oral information according to point 5, oral information according to point 6 and oral explanation according to point 7 free of charge. If, despite obtaining oral certificates, information or explanations under items 2, 5, 6 and 7 of the first paragraph of Article 30 of this Act, an individual requests a certificate, information or explanation in writing, the personal data controller must provide it.

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

The right to supplement, correct, block, delete and object

Article 32

(1) The controller of personal data must, at the request of the data subject, supplement, correct, block, delete or delete personal data which the individual proves to be incomplete, inaccurate or out of date or to have been collected or processed contrary to by law.

(2) The personal data controller must, at the request of the individual, inform all personal data users and contractual processors to whom he provided personal data before the measures referred to in the previous paragraph were implemented, of their completion, correction, blocking or deletion under the previous paragraph. Exceptionally, he does not need to do this if it would result in high costs, disproportionate effort or 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 have the right to demand the termination of their processing at any time with an objection. The administrator grants the objection if the individual proves that the conditions for processing under the fourth paragraph of Article 9 or under 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 does not satisfy the objection referred to in the preceding paragraph, the individual who filed the objection may request that the processing in accordance with the fourth paragraph of Article 9 or the third paragraph of Article 10 of this Act be decided by the National Supervisory Authority. An individual may submit a request within seven days from the service of the decision on the objection.

(5) The state supervisory body for the protection of personal data shall decide on the request referred to in the preceding paragraph within two months of receiving the request. The

submitted request suspends the processing of personal data of the individual in respect of which he / she submitted the request.

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

Procedure for supplementing, correcting, blocking, deleting and objecting

Article 33

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

(2) The personal data controller must supplement, correct, block or delete personal data within 15 days from the day of receipt of the request and inform the applicant or inform him within the same period of reasons why he will not do so. He must decide on the objection within the same time limit.

(3) If the personal data controller does not act in accordance with the preceding paragraph, the request shall be deemed to have been rejected.

(4) If the personal data controller establishes that personal data are incomplete, inaccurate or out of date, it shall supplement or correct them and inform the individual thereof, unless otherwise provided by law.

(5) The costs related to the supplementation, correction and deletion of personal data, the notification and the decision on the objection shall be borne by the personal data controller.

Judicial protection of individual rights

Article 34

(1) An individual who establishes that his rights determined by this Act have been violated may request judicial protection for the duration of the violation.

(2) If the violation referred to in the preceding paragraph has ceased, the individual may file an action to establish that the violation existed if he or she has not been provided with other judicial protection in connection with the violation.

(3) In the proceedings, the competent court shall decide in accordance with the provisions of the law governing administrative disputes, insofar as this law does not provide otherwise.

(4) The public is excluded in the proceedings, unless the court decides otherwise on the proposal of an individual for justified reasons.

(5) The procedure is necessary and a priority.

Interim injunction

Article 35

In a lawsuit filed for violation of the rights referred to in Article 32 of this Act, the individual may request the court to order the personal data controller until a final decision in an administrative dispute to prevent any processing of disputed personal data. the damage to which they relate is irreparable damage, and the postponement of processing is not contrary to the public interest and there is no risk of major irreparable damage to the counterparty.

Restriction 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 restricted by law for reasons of protection of sovereignty and defense of the state, protection of national security and constitutional order, security, political and economic interests the exercise of police powers, the prevention, detection, detection, proof and prosecution of criminal offenses and misdemeanors, the detection and punishment of breaches of ethical standards for certain professions, for monetary, budgetary or fiscal reasons, to control the police and protect the individual concerned 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 Personal Data Protection

Supervisory Authority

Article 37

(1) The state supervisory body for the protection of personal data (hereinafter: the state supervisory body) has the position of the supervisory body for the protection of personal data.

(2) The state supervisory body shall perform inspection supervision over 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 export of personal data from the Republic of Slovenia. The state supervisory body also performs other tasks in accordance with the law.

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

Position and organization of the state supervisory body

Article 38
(expired)

Funds for the work of the state supervisory body

Article 39
(expired)

Appointment of the Chief State Superintendent

Article 40
(expired)

Dismissal of the Chief State Superintendent

Article 41
(expired)

Replacement of the Chief State Superintendent

Article 42
(expired)

Supervisor

Article 43
(expired)

Independence of supervisors

Article 44
(expired)

Employment and assignments to the state supervisory body

Article 45
(expired)

Chapter 2
Tasks of the state supervisory body

Reports of the state supervisory body

Article 46
(expired)

Cooperation with other bodies

Article 47

In its work, the state supervisory body cooperates with state bodies, competent bodies of the European Union for the protection of individuals with regard to the processing of personal data, international organizations, foreign supervisory bodies for personal data protection, institutes, associations, non-governmental organizations in the field of personal data protection and privacy. and authorities on all matters relevant to the protection of personal data.

Competence powers

Article 48

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

(2) **(expired)** .

Public work

Article 49

(1) The state supervisory body may:

1. publishes an internal newsletter and professional literature;
2. publishes 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; ;
3. publish the requests referred to in the second paragraph of Article 48 of this Act on the website or in another appropriate manner after they have been received by the Constitutional Court;
4. publish on the website or in another appropriate manner the decisions and resolutions of the Constitutional Court on the requirements referred to in the second paragraph of Article 48 of this Act;
5. publish on the website or in any other appropriate manner the decisions and rulings of courts of general jurisdiction and the administrative court relating to the protection of personal data, so that personal data of clients, victims, witnesses or experts cannot be deduced from them;
6. give non-binding opinions on the compliance of codes of professional ethics, general business conditions or their proposals with regulations in the field of personal data protection;
7. give optional opinions, explanations and positions on issues in the field of personal data protection and publish them on the website or in another appropriate way;
8. prepares and gives optional instructions and recommendations regarding the protection of personal data in a particular field;
9. make public statements on inspections carried out in individual cases;
10. conducts press conferences related to the work of the state supervisory body and publishes transcripts of statements or recordings of statements from press conferences on its website;
11. publishes other important notices on the website.

(2) In order to exercise the powers referred to in items 6, 7 and 8 of the previous paragraph, the state supervisory body may also invite representatives of associations and other non-governmental organizations in the field of personal data protection, privacy and consumers to participate.

Chapter 3
Inspection

Application of the law governing inspections

Article 50

The provisions of the law governing inspections shall apply to the performance of inspections under this Act, insofar as this Act does not provide otherwise.

Scope of inspection

Article 51

Within the framework of inspection supervision, the state supervisory body shall:

1. control the legality of the processing of personal data;
2. supervise the adequacy of measures for the protection of personal data and the implementation of procedures and measures for the protection of personal data pursuant to Articles 24 and 25 of this Act;
3. supervise the implementation of the provisions of the law governing the catalog of personal data files, the register of personal data files 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 transfer to foreign users of personal data.

Direct inspection

Article 52

(1) Inspection supervision shall be performed directly by the supervisor within the limits of the competence of the state supervisory body.

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

Powers of the supervisor

Article 53

When performing inspections, the supervisor is entitled to:

1. to review documentation relating to the processing of personal data, regardless of its confidentiality or secrecy, and the export of personal data to a third country and the transfer to foreign users of personal data;
2. review the content of personal data files, regardless of their confidentiality or secrecy, and catalogs of personal data files;
3. review the documentation and acts governing the protection of personal data;
4. inspect the premises where personal data, computer and other equipment and technical documentation are processed;
5. check measures and procedures for the protection of personal data and their implementation;
6. exercise other competencies determined by the law governing inspection supervision and the law governing the general administrative procedure;
7. perform other matters determined by law.

Inspection measures

Article 54

(1) A supervisor who, in the course of an inspection, establishes a violation of this Act or another law or regulation governing the protection of personal data, shall have the right to immediately:
1. order that the irregularities or deficiencies which it finds be remedied in a manner and within a time limit which it shall determine;
2. order a ban on the processing of personal data to persons in the public or private sector who have not provided or do not implement measures and procedures for the protection of personal data;
3. order a ban on the processing of personal data and the anonymisation, blocking, deletion or destruction of personal data when it establishes that personal data are being processed in contravention of the provisions of the law;
4. order a ban on the export of personal data to a third country or their transfer to foreign users of personal data if they are exported or transferred in contravention of the provisions of law or a binding international treaty;
5. order other measures determined by the law governing inspection supervision and the law governing the general administrative procedure.

(2) The measures referred to in the preceding paragraph may not be ordered against a person who provides data transmission services in the electronic communications network, including temporary data storage and other actions related to data which are mainly or entirely in the function of performing or facilitating data transfer networks if that person has no interest in the content of that information and is not a person who can effectively control access to that information alone or in conjunction with a limited number of related persons.

(3) If the supervisor establishes during the inspection that there is a suspicion of committing a criminal offense or misdemeanor, he shall file a criminal complaint or carry out procedures in accordance with the law governing misdemeanors.

Judicial protection

Article 55

There is no appeal against the decision or resolution of the supervisor referred to in the first paragraph of Article 54 of this Act, but an administrative dispute is allowed.

Notifying the applicant

Article 56

The supervisor is obliged to inform the notifier about all important findings and actions in the inspection procedure.

Competences of the state supervisory body regarding access to public information

Article 57
(expired)

Secrecy

Article 58

(1) The supervisor is obliged to protect the confidentiality of personal data with which he becomes acquainted during the performance of inspection supervision, even after the termination of the performance of the service of the supervisor.

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

Chapter 4
Cooperation and external control in the field of personal data protection

Ombudsman

Article 59

(1) The ombudsman (hereinafter: the ombudsman) shall perform his / her duties in the field of personal data protection in relation to state bodies, bodies of self-governing local communities and holders of public authority in accordance with the law governing the ombudsman.

(2) The protection of personal data is a special area of the Ombudsman for which one of the Deputy Ombudsmen is in charge.

Annual Report

Article 60

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

Competence of the National Assembly

Article 61

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

PART V
EXPRESSION OF PERSONAL DATA

Chapter 1
Export of personal data to the Member States of the European Union and the European Economic Area

Free movement of personal data

Article 62

Where personal data are transferred to a personal data controller, contractual processor or user of personal data established, established or registered in a Member State of the European Union or the European Economic Area or otherwise subject to its legal order, the provisions of this Act shall not apply. export of personal data to third countries.

Chapter 2
Export of personal data to third countries

General provision

Article 63

(1) The transmission of personal data which are or will be processed only after the transmission to a third country is permissible in accordance with the provisions of this Act and provided that the state supervisory authority issues a decision that the country to which they are exported provides 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 for which it has been established that they fully ensure an adequate level of personal data protection.

(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 partially ensure an adequate level of personal data protection. the purposes for which the appropriate level of protection is established.

The process of determining the appropriate level of personal data protection

Article 64

(1) The state supervisory body shall establish a procedure for determining the appropriate level of personal data protection in a third country on the basis of inspection findings or on the proposal of a natural or legal person who may show a legal interest in issuing a decision.

(2) At the request of the state 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 state ensures an adequate level of protection of personal data.

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

(4) The state supervisory body shall issue a decision within two months of receiving the complete information referred to in the second and third paragraphs of this Article. It can also issue a decision only on a certain type of personal data or their processing for a certain purpose.

(5) The state supervisory body shall be obliged to notify the competent body of the European Union in writing no later than 15 days from the issuance of the decision that the third country does not ensure an adequate level of personal data protection.

Judicial protection

Article 65

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

List

Article 66

(1) The state supervisory body shall keep a list of third countries for which it has established that they have, in whole or in part, an adequate level of protection of personal data or that they do not have such data. If it is established that the 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 ensured.

(2) The Chief State Supervisor shall publish the list referred to in the preceding paragraph in the Official Gazette of the Republic of Slovenia.

Involvement of the state supervisory body in decision - making

Article 67

In its decision-making, the national supervisory authority is bound by the decisions of the competent body of the European Union regarding the assessment of whether third countries ensure 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 state supervisory body is obliged to establish all the circumstances related to the export of personal data. In particular, it must take into account the type of personal data, the purpose and duration of the proposed processing, the legislation in the country of origin and the recipient country, including the personal data protection regime of foreign nationals, and the personal data protection measures used.

(2) In deciding on the previous paragraph, the state supervisory body shall take into account in particular:

1. whether the personal data disclosed are used only for the purpose for which they were disclosed, or the purpose may be changed only with the permission of the controller of personal data provided or with the personal consent of the data subject;
2. whether the data subject has the possibility to find out for what purpose his personal data were used, to whom it was transmitted and the possibility of correcting or deleting inaccurate or out-of-date personal data, unless due to the secrecy of the procedure international treaties;
3. whether the foreign controller implements appropriate organizational and technical procedures and measures to protect personal data;
4. whether a contact person has been appointed who is authorized to provide information to the data subject or to the state supervisory authority on the processing of personal data that have been disclosed;
5. whether a foreign user may disclose personal data only on condition that the other foreign user to whom the personal data will be transferred is provided with adequate protection of personal data also for foreign citizens;
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 shall, with the consent of the Minister responsible for foreign affairs, issue rules specifying which information is considered necessary for the decision of the State Supervisory Authority on the transfer 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 disclosed and transmitted to a third country if:

1. as provided by another law or a binding international treaty;
2. the personal consent of the data subject is given and he or she is aware of the consequences of such transmission;
3. the withdrawal is necessary for the performance of the contract between the data subject and the personal data controller or for the execution of pre-contractual measures taken in response to a request from the data subject;
4. the withdrawal is necessary for the conclusion or performance of a contract concluded between the controller and the third party for the benefit of the data subject;

5. the removal is necessary in order to protect the life or body of the data subject from serious endangerment;
6. withdrawal is made from registers, public books or official records intended by law to provide information to the public and available for public inspection in general or to any person who may have a legal interest in meeting the conditions in a particular case. they are provided for inspection by law;
7. the controller of personal data shall ensure 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 contracts or general terms and conditions.

(2) In the case of the export of personal data pursuant to point 7 of the preceding paragraph, the person intending to disclose personal data must obtain a special decision of the state supervisory body authorizing the export of personal data.

(3) A person may disclose personal data only after receiving the decision referred to in the preceding paragraph, by which the export is permitted.

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

(5) The state supervisory body shall be obliged to forward this to the competent body of the European Union and the Member States of the European Union no later than 15 days from the issuance of the decision referred to in the second paragraph of this Article.

(6) If, after receiving the decision, the competent body of the European Union decides that removal on the basis of the decision referred to in the second paragraph of this Article is inadmissible, the state supervisory body shall be bound by that decision. of this Article, a new decision prohibiting her from further exporting personal data.

Recording the amount

Article 71

The transfer of personal data to 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
OF THE SECTORAL ARRANGEMENT

Chapter 1
Direct Marketing

Rights and duties of the manager

Article 72

(1) The personal data controller may use personal data of individuals collected from publicly available sources or in the course of lawful activities, also for the purposes of offering goods, services, employment or temporary performance of works using postal services,

telephone calls, e-mail or other telecommunication means (hereinafter: direct marketing) in accordance with the provisions of this chapter, unless otherwise provided by other law.

(2) For the purposes of direct marketing, the personal data controller may use only the following personal data collected in accordance with the previous paragraph: personal name, address of permanent or temporary residence, telephone number, e-mail address and fax number. Based on the personal consent of the 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 controller of personal data must carry out direct marketing by informing the individual of his rights under Article 73 of this Act when carrying out direct marketing.

(4) If the personal data controller intends to transfer personal data referred to in the second paragraph of this Article to other users of personal data for direct marketing purposes or to contractual processors, he is obliged to inform the individual and obtain his written consent before providing personal data. The notification to the individual about the intended transfer of personal data must contain information on what data he intends to transfer, to whom and for what purpose. The costs of the notification shall be borne by the controller of personal data.

The right of the individual

Article 73

(1) An individual may at any time request in writing or in another agreed manner that the personal data controller permanently or temporarily ceases to use his personal data for the purpose of direct marketing. The controller of personal data is obliged to prevent the use of personal data for the purpose of direct marketing within 15 days and to inform the individual who requested it in writing or in another agreed manner within the next five days.

(2) The costs of all actions of the personal data controller in relation to 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 implementation of video surveillance, unless otherwise provided by another law.

(2) A person from the public or private sector who performs video surveillance must publish a notice to that effect. The notice must be visibly and clearly published in a way that allows the individual to become acquainted with its implementation at the latest when video surveillance begins to be exercised over it.

(3) The notification referred to in the preceding paragraph must contain the following information:
1. that video surveillance is carried out;
2. the name of the public or private sector person performing it;

3. telephone number for obtaining information on where and for how long the recordings from the video surveillance system are stored.

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

(5) The video surveillance system with which video surveillance is carried out must be protected from access by unauthorized persons.

Access to official office or business premises

Article 75

(1) The public and private sectors may carry out video surveillance of access to their official or business premises, if this is necessary for the safety of people or property, to ensure control of entry or exit into or from office or business premises or if the nature of work employees. The decision shall be taken by the competent official, head, director or other competent or authorized individual of a public sector person or a private sector person. The written decision must explain the reasons for introducing video surveillance. The introduction of video surveillance may also be determined by law or a regulation adopted on its basis.

(2) Video surveillance may be carried out only in such a way that neither the recording of the interior of residential buildings that do not affect the access to their premises nor the recording of entrances to dwellings can be carried out.

(3) All employees in the public or private sector who perform work in the supervised area must be informed in writing about the implementation of video surveillance.

(4) The personal data collection under this Article shall contain a recording of the individual (picture or voice), date and time of entry and exit from the premises, but also the personal name of the recorded individual, address of his permanent or temporary residence, employment, number and type identity document and the reason for entry, if the said personal data are collected in addition to or by recording a video surveillance system.

(5) Personal data referred to in the preceding paragraph may be kept for a maximum of one year after their creation, after which they shall be deleted, unless otherwise provided by law.

Multi-apartment buildings

Article 76

(1) The introduction of video surveillance in a multi-apartment building requires the written consent of the 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 this is necessary for the safety of people and property.

(3) Video surveillance in a multi-apartment building may only control access to the entrances and exits of multi-apartment buildings and their common areas. It is forbidden to carry out video surveillance of the caretaker's apartment and the caretaker's workshop.

(4) It is prohibited to enable or perform real-time or subsequent viewing of recordings of a video surveillance system via internal cable television, public cable television, the Internet or by means of another telecommunication means capable of transmitting such recordings.

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

Workspaces

Article 77

(1) The implementation of video surveillance within work premises may be carried out only in exceptional cases when this is strictly necessary for the security of people or property or for the protection of classified information and business secrets, and this purpose cannot be achieved by milder means.

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

(3) It is prohibited to carry out video surveillance in work areas outside the workplace, especially in changing rooms, lifts and sanitary facilities.

(4) Employees must be informed in writing in advance of the implementation of video surveillance pursuant to this Article.

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

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

Chapter 3
Biometrics

General provision

Article 78

By processing biometric characteristics, the characteristics of an individual are determined or compared, so that his identification can be performed or his identity verified (hereinafter: biometric measures) under the conditions determined by this Act.

Biometric measures in the public sector

Article 79

(1) Biometric measures in the public sector may be determined only by law if this is strictly necessary for the security of people or property or for the protection of classified information and business secrets, and this purpose cannot be achieved by milder means.

(2) Notwithstanding the preceding paragraph, biometric measures may be determined by law if it concerns the fulfillment of obligations under a binding international treaty or the identification of individuals when crossing state borders.

Biometric measures in the private sector

Article 80

(1) The private sector may implement biometric measures only if they are strictly necessary for the performance of activities, for the security of people or property or for the protection of classified information or business secrets. It can only implement biometric measures on its employees if they have been informed 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 implement biometric measures shall submit a description of the intended measures and the reasons for their introduction to the state supervisory authority.

(3) After receiving the information referred to in the preceding paragraph, the state supervisory authority shall decide within two months whether the introduction of biometric measures is intended in accordance with this Act, especially with the conditions referred to in the first sentence of the first paragraph. The time limit may be extended by a maximum of one month if the introduction of these measures would affect more than 20 employees in the private sector or if the representative trade union requires the employer to participate in the administrative procedure.

(4) The personal data controller may implement biometric measures after receiving 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 body referred to in the third paragraph of this Article, but an administrative dispute shall be allowed.

Biometric measures related 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 entering a building or parts of a building and recording the presence of employees at work. .

Chapter 4
Records of entrances and exits from the premises

Evidence

Article 82

(1) A person of the public or private sector may, for the purposes of protecting the property, life or body of individuals and order in his premises, request an individual who intends

to enter or leave this premises to provide all or some personal data referred to in paragraph 2 of this Article; reason for entry or exit. If necessary, he can also check personal data by inspecting the individual's personal document.

(2) Only the following personal data may be kept in the records of entries and exits: personal name, number and type of identity document, address of permanent or temporary residence, employment and date, time and reason for entering or leaving the premises.

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

(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 entry, then deleted or otherwise destroyed, unless otherwise provided by law.

Chapter 5
Public books and protection of personal data

The legal purpose of the public book

Article 83

Personal data from the public book regulated by law may be used only in accordance with the purpose for which they were collected or processed, if the lawful purpose of their collection or processing is determined or determinable.

Chapter 6
Connecting personal data files

Official records and public books

Article 84

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

(2) Controllers or the controller of personal data who connects two or more databases of personal data kept for different purposes shall be obliged to inform the state supervisory body in advance.

(3) If at least one personal data file to be linked contains sensitive data, or if the connection would result in the disclosure of sensitive data or the connection requires the use of the same connection sign, the connection is not allowed without the prior permission of the state supervisory authority. organs.

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

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

Prohibition of association

Article 85

It is prohibited to link personal data files from criminal records and misdemeanor records with other personal data files, and to link personal data files from criminal records and misdemeanor records.

Special provision

Article 86

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

Chapter 7
Expert supervision

Application of the provisions of this chapter

Article 87

Unless otherwise provided by law, the provisions of this chapter shall apply to the processing of personal data in the professional supervision provided for by law.

General provisions

Article 88

(1) A person of the public sector who performs professional supervision (hereinafter: professional supervision provider) may process personal data processed by personal data controllers over whom he has the authority to exercise professional supervision by law.

(2) The provider of professional supervision has the right to inspect, print, transcribe or copy all personal data referred to in the previous paragraph, and is obliged to protect their secrecy when processing them for the purposes of professional supervision and preparing a report or assessment. In the report or assessment at the end of the expert supervision, the provider of professional supervision may record only those personal data that are necessary to achieve the purpose of professional supervision.

(3) The costs of inspection, printing, copying or copying referred to in the preceding paragraph shall be borne by the personal data controller.

Professional supervision and additional processing of personal data

Article 89

(1) When performing professional supervision in which he processes personal data in accordance with the first paragraph of Article 88 of this Act, the provider of professional supervision may inform the data subject in writing that he carries out professional supervision and inform him in writing that he may or give oral views.

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

Professional supervision and sensitive personal data

Article 90

If sensitive personal data are processed during the performance of professional supervision, the provider of professional supervision shall make an official note or other official record in the file of the personal data controller.

VII. PART OF THE CRIMINAL PROVISION

General violations 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, sole proprietor or sole proprietor for a misdemeanor:

1. if he processes personal data without having a basis for this in law or in the personal consent of the individual (Article 8);
2. if he entrusts individual tasks related to the processing of personal data to another person without concluding a contract in accordance with the second paragraph of Article 11;
3. if it processes sensitive personal data in contravention of Article 13 or does not protect it in accordance with Article 14;
4. if it automatically processes personal data in contravention of Article 15;
5. if it collects personal data for purposes that are not specified and lawful, or if it further processes them in contravention of Article 16;
6. if it provides the user of personal data with personal data contrary to the second paragraph of Article 17 or if it does not destroy personal data in accordance with the third paragraph of Article 17 or does not publish the results of processing in accordance with the fourth paragraph of Article 17;
7. if he fails to inform the individual about the processing of personal data in accordance with Article 19;
8. if he uses the same connecting sign contrary to Article 20:
9. if he does not delete, destroy, block or anonymise personal data after the purpose of processing has been fulfilled in accordance with the second paragraph of Article 21;
10. if he acts in contravention of Article 22;
11. if it fails to ensure that the catalog of the personal data file contains data determined by law (Article 26);
12. if it does not provide data for the needs of the register of personal data files (Article 27);

13. if he acts in contravention of 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 in contravention of Article 32 or if he acts in contravention of the second or fifth paragraph of Article 33;
15. if, contrary to the first paragraph of Article 63 or contrary to Article 70, he exports personal data to a third country.

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

(3) A fine of 830 to 2,080 euros shall be imposed on a 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.

(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.

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, sole proprietor or sole proprietor if he exceeds the powers contained in the contract referred to in the second paragraph of Article 11 or does not return personal data in accordance with the third paragraph of Article 11.

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

(3) A fine of 830 to 2,080 euros shall be imposed on a 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.

(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.

Violation of the provisions on personal data protection

Article 93

(1) A fine of 4,170 to 12,510 euros shall be imposed on a legal person, sole proprietor or sole proprietor if he processes personal data in accordance with this Act and fails to provide protection of personal data (Articles 24 and 25).).

(2) A fine of 830 to 1,250 euros shall also be imposed on the responsible person of a legal person, sole proprietor of an individual or an individual who independently performs an activity for the misdemeanor 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 body or a body of a self-governing local community who commits 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.

Infringement of direct marketing provisions

Article 94

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

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

(3) 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.

Violation of general provisions on video surveillance

Article 95

(1) A fine of 4,170 to 12,510 euros shall be imposed on a legal person, sole proprietor or sole proprietor for a misdemeanor:
1. if it fails to publish the notice in the manner referred to in the second paragraph of Article 74;
2. if the notification 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) A fine of 830 to 1,250 euros shall also be imposed on the responsible person of a legal person, sole proprietor of an individual or an individual who independently performs an activity for the misdemeanor 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 body or a body of a self-governing local community who commits 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.

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

Article 96

(1) A fine of 4,170 to 12,510 euros shall be imposed on a legal person, sole proprietor or sole proprietor for a misdemeanor:
1. if it carries out video surveillance without a reasoned written decision or without another legal basis referred to in the first paragraph of Article 75;

2. if it carries out video surveillance by recording the interior of residential buildings that do not affect the access to their premises or recordings of entrances to apartments (second paragraph of Article 75);
3. if he does not inform the employees in writing (third paragraph of Article 75);
4. if he keeps personal data in contravention of the fifth paragraph of Article 75.

(2) A fine of 830 to 1,250 euros shall also be imposed on the responsible person of a legal person, sole proprietor of an individual or an individual who independently performs an activity for the misdemeanor 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 body or a body of a self-governing local community who commits 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.

Violation of the provisions on video surveillance in multi-apartment buildings

Article 97

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

(2) A fine of 410 to 1,250 euros shall also be imposed on the responsible person of a legal person, sole proprietor of an individual or an individual who independently performs an activity for the misdemeanor 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 body or a body of a self-governing local community who commits 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.

Violation of the provisions on video surveillance in the workplace

Article 98

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

(2) A fine of 1,250 to 2,080 euros shall also be imposed on the responsible person of a legal person, sole proprietor of an individual or an individual who independently performs an activity for the misdemeanor 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 body or a body of a self-governing local community who commits an act referred to in the first paragraph of this Article.

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

Violation of public sector biometrics provisions

Article 99

(1) A fine of 4,170 to 12,510 euros shall be imposed on a legal person of the public sector who implements biometric measures in contravention of Article 79.

(2) A fine of 1,250 to 2,080 euros shall also be imposed on the responsible person of a legal person of the public sector for the misdemeanor 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 body or a body of a self-governing local community who commits an act referred to in the first paragraph of this Article.

Violation of biometrics provisions in the private sector

Article 100

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

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

Violation of the provisions on the register of entries and exits

Article 101

(1) A fine of 2,080 to 4,170 euros shall be imposed on a legal person, sole proprietor or sole proprietor for a misdemeanor:

1. who uses the records of entries and exits as official records in contravention of the third paragraph of Article 82;
2. who acts in contravention of the fourth paragraph of Article 82.

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

(3) A fine of 200 to 830 euros shall be imposed on a responsible person of a state body or a body of a self-governing local community who commits 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.

Violation of the provisions on the interconnection of personal data files

Article 102

(1) A fine of 830 to 2,080 euros shall be imposed on a responsible person of a state body or self-governing local community who connects personal data files in contravention of the third paragraph of Article 84.

(2) A fine of 830 to 2,080 euros shall be imposed on a responsible person of a state body or self-governing local community who connects personal data files from criminal records and misdemeanor records with other personal data files or connects personal data files from criminal records with personal files. data from misdemeanor records (Article 85).

Violation of the provisions on professional supervision

Article 103

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

1. if it carries out professional supervision in contravention of the second paragraph of Article 88;
2. if he does not make an official note or other official record in contravention of Article 90 of this Act.

(2) A fine of 830 to 1,250 euros shall also be imposed on the responsible person of a legal person for the misdemeanor 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 body or a body of a self-governing local community who commits 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.

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 OF
TRANSITIONAL AND FINAL PROVISIONS

Powers of the Commissioner for Access to Public Information regarding the Protection of Personal Data

Article 104

(1) An administrative dispute may be initiated against a decision or resolution of a state supervisory body by the Commissioner for Access to Public Information until the enactment of the law regulating this issue, if he assesses that it violates access to public information.

(2) The procedure in the administrative dispute referred to in the preceding paragraph is necessary and priority.

(3) The Commissioner for Access to Public Information shall be obliged to serve on the state supervisory body a decision or resolution in which the Commissioner has commented on the issue of personal data protection.

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 process and collect, with the personal consent of individuals, personal data relating to them, if such data are necessary and appropriate for the performance of their tasks and responsibilities, regardless of the provisions of laws governing their tasks and responsibilities. and the provisions of this Act, pending the enactment of a special law to regulate these matters.

(2) Personal data controllers may disclose and publish the personal name, title or function, business telephone number and business e-mail address of the head and those employees whose work is important due to business with customers or service users, until a special law enters into force. will settle these issues.

The term personal data controller

Article 107

The terms "personal data controller", "data controller" or "database controller" or "database controller", which are defined in the laws, shall be considered the term "personal data controller" under this Act.

Commencement of operation of the National Supervisory Authority for Personal Data Protection

Article 108

(1) The State Supervisory Body for the Protection of Personal Data shall start its work on 1 January 2006.

(2) Until the beginning of the operation of the National Supervisory Body for Personal Data Protection, its competences and tasks under this Act shall be performed by the

Inspectorate for Personal Data Protection of the Republic of Slovenia as a body within the Ministry of Justice and inspectors appointed under the Personal Data Protection Act Nos. 59/99, 57/01, 59 / 01- corr., 52/02-ZDU-1 and 73/04 - ZUP-C).

Appointment of the Chief State Superintendent

Article 109

(1) The procedure for the appointment of the Chief State Supervisor shall begin no later than 1 June 2005.

(2) The term of office of the Chief Inspector for Personal Data Protection shall end on the day of the appointment of the Chief State Supervisor.

(3) If the Chief State Supervisor is appointed before the beginning of the work of the State Supervisory Body for Personal Data Protection, the Chief State Supervisor shall be the head of the Inspectorate for Personal Data Protection of the Republic of Slovenia as a body within the Ministry of Justice.

(4) If the Chief State Supervisor is not appointed by the beginning of the work of the State Supervisory Body for Personal Data Protection, his function shall be performed by the Chief Inspector for Personal Data Protection as acting until the appointment of the Chief State Supervisor.

Acquisition of employees and archives

Article 110

(1) The National Supervisory Body for Personal Data Protection shall take over inspectors and other employees who perform work in the Inspectorate for Personal Data Protection of the Republic of Slovenia on the day of the commencement of the National Supervisory Body for Personal Data Protection.

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

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 come into force on the day of the commencement of operation of the National Supervisory Body for Personal Data Protection.

(2) Until the establishment of the website of the National Supervisory Authority for Personal Data Protection, the information published by the State Supervisory Authority on its website pursuant to this Act shall be published on the website of the Ministry of Justice.

Completion of ongoing procedures

Article 112

If the decision or resolution of the inspector is issued before the entry into force of this Act, the procedure shall be terminated in accordance with the provisions of the Personal Data Protection Act (Official Gazette of the RS, nos. 59/99, 57/01, 59/01 - corr., 52/02 - ZDU- 1 and 73/04 - ZUP-C).

Transfer of management of the register of personal data files

Article 113

(1) Common catalog of personal data kept 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 - amended, 52/02 - ZDU-1 and 73 / 04 - ZUP-C), shall be renamed into the register of personal data collections on the day this Act enters into force.

(2) Until 1 January 2006, the register referred to in the preceding paragraph shall be kept and maintained by the Ministry of Justice, and on that date it shall be submitted to the National Supervisory Body for the Protection of Personal Data.

Supplementing the data in the register of personal data files

Article 114

Personal data controllers 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 - corrigendum, 52/02 - ZDU-1 and 73/04 - ZUP-C) must submit all data referred to in Article 27 of this Act to the competent body referred to in Article 113 of this Act in the joint catalog of personal data 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 shall cease to be in force (Official Gazette of the Republic of Slovenia, Nos. 59/99, 57/01, 59/01 - amended, 52/02 - ZDU-1 and 73/04 - ZUP -C).

(2) The second indent of the first paragraph and the third paragraph of Article 13 of the Decree on Bodies within Ministries (Official Gazette of the Republic of Slovenia, No. 58/03) shall cease to apply on the day the National Supervisory Body for Personal Data Protection begins.

(3) 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) in the part determining the collection, processing and publication of EMŠO - uniform citizen's identification numbers.

Change in second law

Article 116

In the Ratification Act of 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), Article 3 replaces the text "Science and Technology" with the text "Justice «.

Entry into force

Article 117

This Act shall enter into force on 1 January 2005. "

The Information Commissioner Act - ZInfP (Official Gazette of the Republic of Slovenia, No. 113/05) amends Article 104 of the Act to read as follows:

"Competences of the Commissioner for Access to Public Information regarding the Protection of Personal Data

Article 104
(expired) ';

amends Article 108 of the Act to read as follows:

»Commencement of operation of the National Supervisory Authority for Personal Data Protection

Article 108
(expired) ';

amends Article 109 of the Act to read as follows:

“Appointment of the Chief State Superintendent

Article 109
(expired) ';

amends Article 110 of the Act to read as follows:

Acquisition of employees and archives

Article 110

(expired) ';

and contains the following final provision:

»20. member
(entry into force)

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

The Act Amending the Constitutional Court Act - ZUstS-A (Official Gazette of the Republic of Slovenia, No. 51/07) contains the following final provision:

»40. member

This Act shall enter into force on 15 July 2007. "

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

»TRANSITIONAL PROVISION

Article 17

The Minister responsible for justice shall issue the rules referred to in the seventh paragraph of Article 31 of the Act within sixty days of 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 enter into force on the sixtieth day after the publication of this Act. "