INFORMATION
COMMISSIONER

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

342.5:659.2(497.4)

PIRC Musar, Nataša
Vstopite, dostop je prost! : dostop do informacij javnega značaja / [avtorji besedila Nataša Pirc Musar, Simona Rodež ; fotografije Photo Alto]. - Ljubljana : Informacijski pooblaščenec, 2006

ISBN 961-238-586-6
1. Gl. stv. nasl. 2. Rodež, Simona
224571648

Access to my Privacy Denied!

Contents

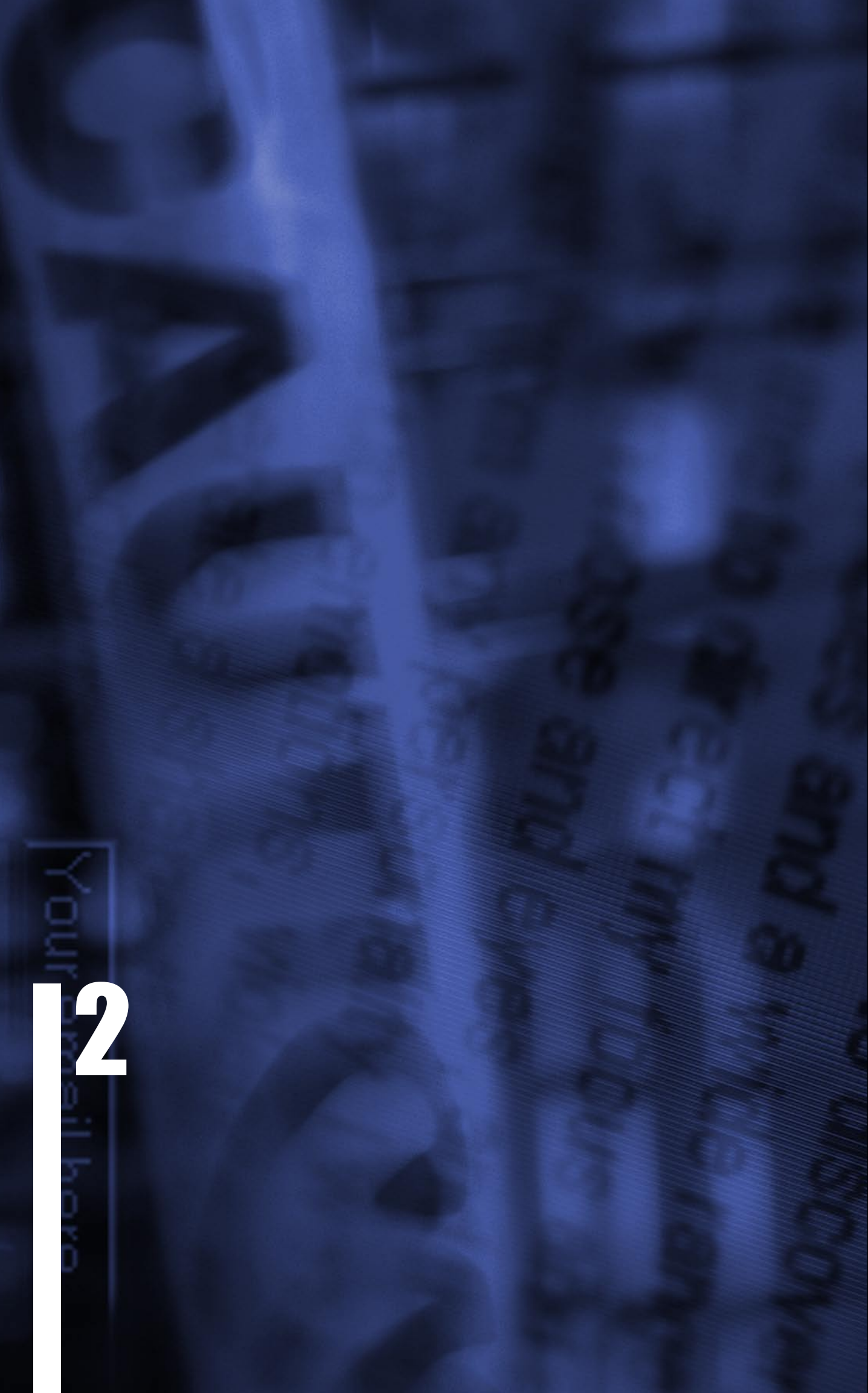
1

The fundamentals of personal data legislation in Slovenia were laid down by the **Constitution** in 1991. Art 38. of the Constitution stipulates the following:

"PROTECTION OF PERSONAL DATA IS ENSURED. THE USE OF PERSONAL DATA, IF IN CONFLICT WITH THE PURPOSE OF DATA COLLECTION, IS FORBIDDEN. COLLECTION, PROCESSING, PURPOSE OF USE, CONTROL AND PROTECTION OF CONFIDENTIAL PERSONAL DATA ARE PROVIDED BY THE LAW. EVERY PERSON HAS THE RIGHT TO BE INFORMED ABOUT PERSONAL DATA COLLECTED RELATED TO HIM AND THE RIGHT TO JUDICIAL PROTECTION IN CASE OF ABUSE OF PERSONAL DATA."

In 1999 a new Personal Data Protection Act (**ZVOP-A**) was adopted, followed by amendments in 2001. **ZVOP-1**, which came into force on January 2005, was harmonised with the European Directive on the Protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/ES).

With the **Act on Information Commissioner**, which came into force on Dec 31, 2005, a new state body, i.e. Information Commissioner, was established. Being an independent state body, the commissioner's authority is now to control the protection of personal data as well.



2

Dear readers,

The rights to freedom of speech, as well as protection of privacy and access to information are already provided by the constitution. So we can say that these rights have been put into the cradle of all citizens of Slovenia. These rights signify the basic principles of democracy which are implemented by the Access to Public Information Act and Personal Data Protection Act. Public sector officials of the Republic of Slovenia need to be aware that both, access to public information, and protection of privacy are the common rights of people. And it is for this reason that we need to take this as a challenge, to respect these rights and to do everything to enable the citizens to exercise these rights and implement the law.

I am glad to say that as early as 2003, Slovenia got a good, modern law on access to public information, followed by amendments in 2005. It goes without saying that the law brought about new thinking and new values to the work of public administration. Since then we have become aware how important it is and what positive effects it has had on the quality of life and democracy in general. Not so long ago some public officials acted with superior arrogance, thinking that no-one has the right to ask for information. But that has dramatically changed and we are now aware that all information, except some exemptions, is public.

When the Act on Information Commissioner was adopted in 2003, which extended the competencies of the Commissioner to the protection of personal data, our office had to start focussing more on the issues of the protection of privacy. We found out that in fact one third of the cases that we had dealt with in relation to access to public information it was a question of conflicts between the right to know and the right to privacy, which are actually two sides of a coin. Now, that the competencies have extended from public sector to the surveillance of personal data processing, we have moved into the private sector, which means dealing with approximately 100.000 entities of private law.

Thus, with information, which on the one hand is open, and the surveillance and protection of personal data on the other, we can now ensure that natural and juristic persons can now enjoy their basic human rights.

The team of the Commissioner's office are aware of the responsibilities we have been entrusted in weighing between the rights of the applicants and persons under obligation, and between the right to access information and protection of privacy. Our team is not large but we are available for information to all applicants, and other colleagues from public administration offices, and private sector. We like to be challenged and are ready to cooperate. We are all striving to make the society happier with what we can do and what we know.

This brochure had been made to give some insight into the protection of personal data. I hope the information contained in it will help you better understand the area and help you in the future to make easier, quicker and better and more professional decisions.

Nataša Pirc Musar,

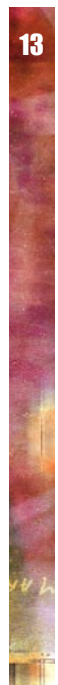
Information Commissioner

Stan Items Tool

3

The need to protect privacy first emerged as a reaction to telephone bugging and other forms of breaking into the private field of individuals. The right of personal data protection started emerging with the advent of modern technologies which created numerous possibilities for breaking into the privacy by means of telephone bugging, installing tapping devices, and other media for disseminating information (video cameras, computers, etc). Before this, people were almost sure that they could not be eavesdropped in their private premises. Having control over a large group of people was much more difficult then since the information was scattered and difficult to access. Thus the need for legislation which would protect personal data came rather late and it was introduced simply to achieve balance between the right to privacy and introducing legitimate reasons for the use of personal data. There was a need for such legislation which would protect the rights of individuals, while at the same time enabling the collection and processing of these data to those subjects who for some legitimate reason need this information.

The first laws related to the protection of personal data in **Europe** started emerging in the 70's in the 20th century. Sweden was the first country in the world which adopted the law on personal data protection in 1973 and has rich experience in this field. In addition to the law from 1998 protection of personal data in Sweden is regulated by numerous other sector-specific laws which need to comply with the system legislation. Thus constant alignment with the system legislation is provided. Following the example of Sweden, similar acts were adopted in Greece, Hungary, France and Finland, and in 1984 also UK and Northern Ireland. The most significant development of legislation in this field started in the 90's when European countries, one by one, adopted similar laws (Germany, Slovakia, Austria, Denmark, Italy, Norway and others). At the turn of the century this legislation was harmonised with the provision of the European Directive 95/46/ES.



4

To better understand the field of personal data protection it is necessary to know the meaning of some basic concepts, used in ZVOP-1.

The definition of **personal data** encompasses a rather large field and includes any data related to individuals, irrespective of the form in which it is expressed.

An **Individual** is someone identifiable as a physical person to whom personal data relates; it is identifiable (by the use of unique personal code EMŠO, or tax number), or one or more factors typical for individual's physical, physiological, mental, economic, cultural or social identity provided the method of identification does not incur large costs or disproportionate effort or require a large amount of time.

Processing of personal data means any activity related to personal data, particularly collection, acquisition, disclosure by transmission, communication, dissemination or otherwise making available, alignment or linking, anonymising, erasure or destruction; processing may be performed manually or by using information technology. Since the meaning of the term is broad, one should understand the concept of personal data protection, meaning that in particular, it is forbidden to use personal data which is in contrast with the purpose of collecting the data, which needs to be defined in advance.

Filing system

is a structured set of data, containing at least one piece of personal data organised in such a manner as to identify or enable the identification of an individual.

Register of filing systems

is a register containing data from filing system catalogues.

Filing system catalogue

is a description of a filing system.

Data controller

is a natural person or legal person or other public or private sector person which by law or by written consent of an individual is authorised to set up, maintain and control the personal data filing system. A contractual data processor may perform these duties on behalf of, or for the account of the data controller.

Personal data recipient

is a natural or legal person, or other private of public sector person to whom the data are supplied and disclosed.

Personal consent of an individual

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

Written consent of an individual

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

Oral consent or other appropriate consent

is a consent given orally, or by means of telecommunication or other appropriate means from which it can be concluded unambiguously that the individual has given his/her consent.

Blocking

means labelling of personal data to restrict or prevent their further processing.

Anonymising

is alteration of personal data in such a way that they can no longer be linked with an individual.

Sensitive personal data

are data on racial, national or ethnic origin, political religious or philosophical beliefs, trade-union membership, health condition, sexual orientation, entry in, or removal from criminal records or offences that are kept on the basis of the law that regulates offences, biometric characteristics if their use makes it possible to identify an individual in connection with any of the circumstances mentioned before.

General legal aspects of personal data protection

In principle the law stipulates that the function of personal data protection is to prevent illegal and unjustified encroachment into the privacy of individuals in all relevant fields. The law stipulates that the protection of personal data is provided to every person in Slovenia, regardless of the citizenship or place of residence.

Personal data need to be processed legally and in good faith and be suitable in terms of scope and purpose of use for which they have been collected and further processed. It is also important to follow the principle of prohibiting discrimination by which every person has the right for his personal data to be protected regardless of any personal circumstance.

It is important that both, public and private sector are treated differently in legal terms when personal data processing is in question. Legal grounds pertaining to the public sector are more restrictive: this sector is allowed to process personal data only if defined by the law. This means that some data may be processed only upon previous personal consent. State bodies, local community bodies and public powers holders have only a limited scope of the use and processing of personal data. If processing of data is legally allowed there is no difference between the private and the public sector: processing is always allowed, however the proportionality factor between processing of personal data and the purpose of processing needs to be taken into account, which also needs to be legally defined.

In private sector personal consent is equal to the provision of the law, since personal data in private sector may be processed if determined by the law and if personal consent of an individual is given.

Due to different legal grounds for processing personal data in public and private sector it is necessary to be aware of these and emphasize them, particularly for the reason because ZVOP-1 and Access to Pubic Information Act define persons differently. According to ZVOP-1 public sector persons can also be subjected to ZDIJZ: legal and natural persons, performing public services, pubic commercial institutions and public enterprises. Different definitions of the public sector used in the ZDIJZ and ZVOP-1 require a different approach, meaning also, that the judicial status of personal data controllers and individuals is different.

According to the law, legal or natural persons performing jobs in public services, or any activities from the act governing companies, can now directly process personal data of individuals who are in contractual relationship with them according to ZVOP-1, but only if personal data are needed for the fulfilment of contractual obligations, or for enforcing the rights stemming from the contractual relationship.

An individual, whose personal data are being processed based on his/her consent, needs to be notified in writing about the purpose of data processing, its use and duration of storage of the data.

Judicial protection of individuals is provided by the Constitution of RS (Art 38). ZVOP-1 contains a number of provisions which prevent the abuse of personal data, thus minimising the need for judicial protection.

Accuracy and up-to-dateness of personal data

One of the provisions requires that personal data being processed must be accurate and kept up-to-date. Thus a data controller may check the accuracy before entering data into the system, either by examining an identity document or suitable public document of the individual to whom the data relate.

Informing the individual of the processing of personal data

Whenever personal data are processed, the individual has the right to be informed about the data controller or its legal representative (personal name, title or official name and address or seat), and the purpose of the processing of personal data.

Use of the same connecting code

There is a provision which prevents the abuse of personal data by using the same connecting code during the acquisition of personal data from filing systems in the field of health, police, national intelligence security activities, national defence, judiciary and state prosecution and criminal record and minor offence records. The same connecting code may exceptionally be used for acquiring personal data if this is the only item of data in a specific case that can help detect criminal offence to protect the life and body of an individual, or to ensure the implementation of the tasks of intelligence and security bodies. In this case an official annotation or other written record must be made.

Duration of storage of personal data

In order to avoid the abuse, the moment the purpose of processing personal data is completed, the data need to be erased, destroyed, blocked, or anonymised unless they are defined as archive materials, or if defined otherwise by the law.

Supply of personal data

Personal data may be collected also for the purpose of supplying the data to authorised users. In this case the data controller must supply the data against payment. By special provision the data controller of the Central population register or Records of permanently or temporarily registered residents are obliged – if there is a legal interest for exercising the rights before pubic sector – to supply the name and address of permanent or temporary residence of an individual against whom the rights are exercised. This provision is mostly used in cases of judicial procedures.

In any case, for each data supply, the data controller needs to provide the so called tracking, meaning that later, it is always possible to find out what personal data, to whom, when and on what basis have been supplied. This period

must cover the time given by statutory protection of the rights of an individual due to non-allowed supply of personal data.

The procedure is less strict in supplying personal data when both, the data controller and the user of data are from public sector. In this case personal data are supplied without payment. A supply, free of charge, is also provided in cases when data are used for historical, statistical or scientific-research purposes.

Protection of personal data of deceased individuals

Protection of personal data does not cease after death. The data controller is allowed to supply personal data about a deceased person only to legally authorised users. Also, the data may be supplied to the legal hairs of the first or second order or if they demonstrate a lawful interest provided that the deceased person did not prohibit in writing the supply of such data. The data controller may supply such data for historical, statistical, or scientific-research purposes, however, only if the deceased individual, or heirs of first or second order have not prohibited in writing the supply of these data.

Security of personal data

The provisions related to the security of personal data represent technical aspect of the law, including logical-technical procedures and measures for protecting personal data. The purpose of providing security is to prevent accidental or deliberate unauthorised destruction, modification or loss of data, preventing alterations, or the loss or unauthorised processing of such data. Security is provided by:

1. protecting premises, equipment and system software,
2. protecting software applications used to process personal data,
3. preventing unauthorised access to personal data during transmission, including transmissions via telecommunications networks,
4. ensuring effective methods of blocking, destruction or anonymisation of personal data,
5. ensuring effective methods for blocking, destruction or anonymisation of personal data,
6. enabling subsequent determination of when personal data were used or entered into the filing system, who did so, for the period covered by legal protection of rights. This allows for tracking the use of data which is one of the provisions of the protection of an individual. If data are accessible via telecommunication networks, all the equipment must ensure that the processing of data is within the limits of authorisation of the users of data. All persons coming in contact with personal data must protect their secrecy and this is binding also after the termination of their functions or jobs.

Both, data controllers and contractual data processors, need to ensure the protection of personal data. Since security of personal data is the most important provisions for preventing the abuse, data controllers must define procedures and measures in their internal acts and appoint persons who are responsible for this field.

Every individual has the right to know who, in what manner and for what purpose his/her personal data are processed. ZVOP stipulates that every personal data controller needs to establish a filing system catalogue for each filing system, including:

1. *title of the filing system,*
2. *information on the data controller (for natural person: personal name, address where activities are performed or address of permanent or temporary residence, and for sole traders his/her company name, seat and registration number; for legal entities: title or registered office of the personal data controller and registration number,*
3. *legal basis for processing personal data,*
4. *category of individuals to whom the personal data relate,*
5. *types of personal data in the filing system,*
6. *purpose of processing,*
7. *duration of storage of personal data,*
8. restriction of the rights of individuals with regard to personal data in the filing system legal basis for such restrictions,
9. *users or categories of users of personal data contained in the filing system,*
10. *information whether personal data are transferred to a third country, to where, to whom and the legal grounds for such transfer,*
11. *general description of the security of personal data,*
12. *data on linked filing systems from official records and public books,*
13. *data on the representative from Par. 3, Art. 5 of this Act (for natural persons: personal name, address where activities are performed and address of permanent or temporary residence; for sole traders: his/her official name, seat and registration number; for legal persons: title or registered office and address of seat of the data controller and registration number).*

The data controller must ensure that the contents of the catalogue is accurate and up-to-date.

Notification of the supervisory body for the needs of the register

The data controller must supply data mentioned in the previous paragraph to the Information Commissioner (see subparagraphs marked bold) at least 15 days prior to establishing a filing system or entering a new type of personal data. Each modification needs to be notified within 8 days at the latest. This does not apply to the filing systems which are maintained for the employees in accordance with the statutes governing filing system in the area of labour, provided that there are less than 20 employees on permanent contract basis.

Based on this information the Information Commissioner establishes and maintains a register of filing systems, using the methodology for its management. This is regulated by special rules. The register is published on the website of the Information Commissioner together with the instructions for registering a filing system.

Examination of the Register

According to ZVOP-1, the Information Commissioner is obliged to permit anyone to examine the register of filing systems and to transcribe the data. The examination and transcription must be permitted and enabled as a rule on the same day, or within 8 days at the latest, otherwise the request is deemed to have been refused. Since the Commissioner needs to publish the register on the website, this right of an individual is exercised only in case the individual does not have access to the web.

Right of the individual to information

Based on the rights of an individual to be informed about his/her own personal data, the data controller is obliged on request of an individual to:

1. enable to examine the filing system catalogue,
2. to certify whether the data relating to him are being processed or not and to enable to examine, transcribe or copy the data,
3. supply the extract of personal data relating to him,
4. provide a list of data recipients to whom the data have been supplied, when, on what basis and for what purpose,
5. provide information about the sources on which data in the filing system are based and methods of processing,
6. provide information on the purpose of processing and types of personal data being processed,
7. explain technical or logical-technical procedures of decision-making if automated decision-making is being used.

This right can be exercised by filing a request, either in writing or orally in an annotation with the data controller. The data controller must enable the individual to examine, transcribe or copy personal data within 15 days from the date of receipt of the request, or notify the individual on the reasons why the examination or copying is disabled. It is also possible to request the extract of personal data and the list of users; however the deadline is longer, i.e. 30 days. If the data controller does not notify the individual within the prescribed period of time, the request is deemed to have been refused. If the data controller does not supply personal data to the individual can file an appeal with the Information Commissioner.

Right to supplement or correct personal data

In order to keep the data accurate and up-to-date, the data controller is obliged on request of an individual to supplement, correct, block or erase personal data which the individual proves as being incomplete, inaccurate, or not up-to-date, or that the data have been collected or processed contrary to the law. On request of the individual the data controller must inform all data recipients and contractual data processors to whom the data have been supplied. Exceptionally, this is not required if it would incur large costs, or require disproportionate efforts in terms of money and time. The request must be lodged in writing or orally in an

annotation with the data controller. All alterations must be done within 15 days from the receipt of the request and the applicant needs to be notified on the reasons for refusing the request. In case of silence the request is deemed to be refused. Costs relating to the alteration are borne by the data controller. If the data controller finds out on his own that the data are incomplete, inaccurate or not up-to-date, the controller is obliged to supplement and correct them. The individual must be notified if not otherwise stipulated by the law.

Exceptionally, personal data in the public sector can also be processed if not explicitly stated by the law and if processing such data is necessary for implementing legal competencies, tasks and activities in the public sector and if this encroachment does not affect legal interest of the individual to whom the data are related. Similarly, personal data may be processed in private sector if this is necessary in order to realise legal interests of the private sector and if these interest overrule the interests of an individual to whom these data are related. In such cases an individual can prove the data controller that the conditions for exceptional processing of personal data have not been met and can request the cessation of processing of his/her personal data. If the data controller refuses the request, the individual may file an appeal with the Information Commissioner. The appeal must be filed within 7 days from receiving the decision on refusal, and the Information Commissioner needs to bring a decision within two months from the receipt of the appeal. During this period personal data processing of the individual needs to be stopped and the costs are borne by the data controller.

Judicial protection of an individual

Judicial protection is ensured by the Constitution of RS, and is further regulated in more detail by ZVOP-1. Thus, an individual, if it is found out that his/her rights have been violated, can request judicial protection for the period until a final decision is issued. If the violation has terminated, the individual may file a suit to find out whether the violation of the rights existed and if no other judicial protection was provided related to the dispute. The appeal is processed by the administrative court if not stipulated otherwise by the personal data protection act. The procedure is treated as an urgent case, meaning that the court needs to bring a decision in the shortest time possible. The proceeding is generally not public. The law also allows issuing a temporary injunction, by which an individual may request the court to bind the data controller to stop processing the disputed personal data until a final decision in the administrative dispute is issued.

Restriction of the rights of an individual

It is possible to restrict the rights of an individual by using a proportionality test. Exceptionally, it is possible to restrict only the following rights of individuals:

- informing the individual on processing of personal data,
- informing the individual about own personal data,
- supplementing, correcting, blocking, erasing or objection.

The above mentioned rights are restricted only by the statute for the reasons of the protection of national sovereignty and national defence, protection of national security and the constitutional order of the state, security, political and economic interests of the state, exercising the responsibilities of the police, prevention, discovery, detection, proving and prosecution of criminal offences and minor offences, the discovery and punishment of violations of ethical norms for certain professions, for monetary, budgetary or tax reasons, supervision of the police, and protection of the individual to whom the personal data relate, or the rights and freedoms of others. However, these restrictions may only be determined within the scope, necessary to achieve the purpose for which the restriction was provided.

Supervisory body – Information Commissioner

When the Act on Information Commissioner came into force, a new, independent state body, the Information Commissioner was established. It has numerous competencies in the field of personal data protection and access to public information. Among others, it is authorised to supervise the implementation of the Personal Data Protection Act and other regulations in the field. The body is headed by the Information Commissioner, who is simultaneously also the principal state supervisor for the protection of personal data. The basic tasks of the Information Commissioner are to ensure uniform implementation of the measures related to personal data protection and to cooperate with the ministries during the preparatory phase of legislation pertaining to the field.

Within the scope of inspection supervision, the Information Commissioner is responsible to supervise:

1. the legality of personal data processing,
2. suitability of measures and procedures for the protection of personal data,
3. implementation of the provisions of the law governing filing system catalogue, register of filing systems, and keeping records on supplying personal data to individual recipients,
4. implementation of the provisions of the law related to the supply of data to a third country and supply to foreign recipients.

The competencies of the state supervisor are the following:

1. examining the documentation relating to the processing of personal data, regardless of the confidentiality or secrecy, transfer of personal data to third countries and the supply to foreign recipients,
2. examining the content of the filing systems and filing system catalogues irrespective of their confidentiality or secrecy,
3. examining the documentation and acts regulating the security of personal data,
4. examining the premises in which personal data are processed, computers and other equipment and technical documentation,
5. verifying measures and procedures for securing personal data and their implementation,
6. exercising other competencies provided by the law governing inspection supervision and the law governing general administrative procedures.
7. performing other duties provided by the law, in particular the law on inspection supervision.

The state supervisor, when during performing inspection supervision, detects a violation of the law or some other regulation governing the protection of personal data, has the right to immediately order the following measures:

1. to eliminate the irregularities or deficiencies in the manner and within the time interval he/she defines,
2. to order the prohibition of personal data processing to persons in the public

or private sector who have failed, or do not implement the measures and procedures to secure personal data,

3. to prohibit the processing of personal data and their anonymisation, blocking, erasing, or destruction, if processed contrary to the provisions of the law,
4. to prohibit the transfer of personal data into a third country, or the supply of data to third foreign recipients if this is against the provisions of an international agreement,
5. to order other measures provided by the laws covering the inspection supervision and general administrative procedure act.

There is no appeal against the decision of the supervisor, but an administrative dispute is permitted. If the supervisor establishes that there is a suspicion of a criminal offence, the commissioner must lay information or implement a procedure according to the law governing offences.

Cooperation with other bodies

The Information Commissioner cooperates with other state bodies, bodies of the European Union for the protection of personal data, international organisations and other supervisory bodies for the protection of personal data, institutions, associations, non-governmental organisations in the field of personal data or privacy protection, and other institutions or bodies in all fields related to personal data protection.

Competencies related to regulations

Information Commissioner also gives preliminary opinions to the ministries, to the National Assembly, self-governing local community bodies and holders of public powers on the questions of conformity of the proposals of statutes and regulations with the legislation regulating personal data protection. If there are doubts regarding the constitutionality related to the procedures that are run by the Commissioner's office, the Commissioner can file a request to review the constitutionality of the proposed legislation.

Publicity of work

The work of the Commissioner is public, thus the information about the activities can be published in newsletters, professional literature, etc. Preliminary opinions, requests for the review of the constitutionality (after they have been received by the court), the Commissioner's conclusions and decisions can be published on the web site. The same goes for the decisions of the courts with general and administrative competence, which relate to the protection of personal data. The Commissioner also gives non-compulsory opinions on the conformity of the code of professional ethics, general conditions of management or proposals for regulations in the field of personal data protection. Also, the Commissioner can issue non-compulsory opinions, explanations, instructions,

recommendations and views on the questions related to the protection of personal data and give press releases on the completed inspector supervisions to the media.

If you visit the web site you will find under Decisions - Personal data protection all the decisions issued by the Commissioner. Using a browser, you can find documents by content or by date.

Transfer of personal data to European Union (EU) or European economic area (EEA) or third countries

The Slovenian Personal Data Protection Act is now harmonised with the legislation of other EU countries or EEA. The provisions of this Act do not apply to the countries of EU or EEA. Third countries are, according to the definitions of the act, the countries which do not belong to the members of EU or EEA. (EEA countries are Norway, Iceland and Liechtenstein).

Transferring of personal data to a third country is allowed after a decision has been issued by the Information Commissioner that the country, to which the data are transferred, ensures an adequate level of protection of personal data. (Such decision is not required if the third country is on the list of those countries that have been found to fully ensure an adequate level personal data protection). Information Commissioner manages a list of third countries which have been found to ensure fully, or partially an adequate level of personal data protection, and the list of countries which do not ensure such protection. If it is found out that a third country only partially ensures protection, the list includes information on the points which ensure personal data protection. The list is published in the Official Gazette or R Slovenia.

Such a decision is not required also if stipulated by some other law or international agreement, or if the individual gives a written consent for the transfer of his/her data. However, the individual must be notified about the consequences of such data transfer from the country.

Transfer of data is also possible for the purposes of protecting the life or body of an individual in concluding or implementing contracts, which are for the benefit for the individual, and for some other reasons listed in the provisions of the law.

The Information Commissioner must introduce a procedure for establishing the adequate level of personal data protection in a third country using the means of inspector supervision, or upon the motion of a natural or legal person who may express a legal interest for issuing such a decision. In such cases the Commissioner cooperates with the ministry of foreign affairs and the competent body of the EU. If the country does not provide adequate level of personal data protection, the Commissioner must notify the competent body of EU within 15 days from issuing the decision. There is no appeal against such decision, however an administrative dispute is permitted.

When dealing with questions of adequate level of personal data protection in third countries, the Commissioner must carefully examine the type of personal data, the purpose of use and duration of personal data processing, legislation of the country supplying the information and the recipient country, including the question of personal data protection of foreign citizens and measures for the protection of personal data which are used in those countries. The decision must be based on the following:

1. whether the data are used for the purpose they have been transferred, whether the purpose can be changed but only on the basis of a consent of a data controller who has supplied the data, or on the basis of personal consent of an individual.
2. whether the individual can learn for what purpose his/her personal data have been used, to whom they have been supplied, and whether they can be corrected or erased if the data are inaccurate or not up-to-date, if this, because of the confidentiality of the procedure would hinder the realisation of an international agreement.
3. whether a foreign data controller implements corresponding organisational and technical procedures and measures for the protection of personal data,
4. whether an authorised contact person, who can give information on these matter, has been defined,
5. whether a foreign recipient may transfer personal data but only under condition if the other foreign recipient, to whom the data will be supplied to, can provide adequate personal data protection to foreign citizens.
6. whether an efficient legal protection of individuals, whose personal data have been transferred, is provided.

1. Direct marketing

Direct marketing means offering goods, services, employment or temporary performance of work, the use of postal services, telephone calls, electronic mail or other telecommunication means. In a modern consumer society direct marketing is in constant growth. Therefore, it is important that personal data controller uses only those data of individuals that have been collected from publicly available sources or within the scope of its legal authority. For this reason, a data controller may use only the following data: personal name, address of permanent or temporary residence, telephone number, e-mail address, and fax number. On the basis of personal consent of an individual, the data controller may use other sensitive personal data if a personal consent of an individual has been given. The consent is explicit, and as a rule, must be given in writing.

During the performance of direct marketing, the data controller must notify the individual on his/her rights so that the individual can request in writing, or in another manner, a permanent or temporary cessation of the use of his/her personal data for the purposes of direct marketing (the so called "opt out" possibility). The personal data controller is bound to prevent the use of personal data within five subsequent days for the purpose of direct marketing and notify the individual who has so requested within the following five days in writing, or in another agreed manner.

If personal data are supplied to another user, the data controller must notify the individual accordingly, stating what data, to whom and for what purpose they will be used.

2. Video surveillance

Modern information technology development offers numerous possibilities for surveillance. A person who conducts video surveillance must publish a notice to this effect. It must be visible and plainly made public so that individuals can acquaint themselves about its implementation. The notice must contain the following:

1. information that video surveillance is taking place,
2. title of the person in the public or private sector implementing the surveillance,
3. telephone number to obtain information as to where and for which period the records from surveillance will be stored,

The law stipulates that vide surveillance system must be protected against access by an unauthorised person.

a) Official office premises or business premises

Both, public and private sector may implement video surveillance of access to their official office premises or business premises if this is necessary for the security of people and property, for ensuring supervision of entering or exiting, or if due to the nature of the work there exists a potential threat to the employees. The decision must be taken by a competent function-

ary, head director or some other competent individual. The written decision must explain the reasons for the introduction of vide surveillance. Video surveillance may also be laid down by a law or regulation. Video surveillance may be implemented by informing all the employees working in the premises under surveillance, in writing. The filing system of the surveillance must contain a recording of an individual (image, voice), date and time of entry to or exit from the premises, and also the individual's name, address of permanent or temporary residence, employment, the number and type of his/her personal document and the reasons for entry. Personal data may be stored for a maximum of one year from their creation, after which they must be erased unless otherwise provided by the law.

b) Apartment buildings

Nowadays, more and more tenants, living in apartment buildings, decide to introduce video surveillance for the purpose of security. For this reason it must be noted that it is necessary to obtain a written consent of joint owners of more than 70% ownership. Video surveillance in such apartment buildings can be introduced simply to protect the security of people and property. Thus only monitoring the access to entrances and exits and common areas of apartment buildings is allowed. It is forbidden to have video surveillance of the housekeeper's apartment and the workshop of the housekeeper. Also, it is forbidden to enable examination of the recordings of video surveillance through internal cable television, public accessible television, the Internet, or by using other telecommunication means, able to transmit such recordings. It is also forbidden to record entrances to individual apartments.

c) Work areas

Video surveillance may be implemented in work areas but only under conditions and manner stipulated by the law. It can be implemented only in exceptional cases, when necessary for the safety of people or property or for the protection of secret data and trade secrets, and when such purpose cannot be achieved by milder means. For this reason, video surveillance can be implemented only in the parts of work areas where such interests need to be protected. It is forbidden by law to monitor work premises outside work areas, particularly in changing rooms, lifts and sanitary areas. Prior to the introduction of video surveillance in the private or public sector, the employer must consult the trade union representative at the employer.

3. Biometrics

Biometrics means encroachment into a body, since biometric parameters denote physical, physiological and behavioural characteristics of an individual, which are unique and permanent. They allow for the identification of an individual, particularly by finger prints, ridge structures on fingers, iris and retina scans, face, or ear shape analysis, DNK, and characteristic posture of an individual. By processing biometric characteristics it is possible to identify or compare the characteristics of an individual, thus allowing for the identification under the conditions provided by ZVOP-1 (biometric measures).

Biometrics in the public sector may only be provided for by the law if it is necessary to ensure the security of people, property, secret data and trade secrets and when this purpose cannot be achieved by using milder means.

In the private sector biometrics can be implemented for the same reasons as in the public sector if this is necessary for the performance of activities. Biometric measures may only be used on employees if they have been informed in writing. If the implementation of biometric measures in private sector is not regulated by the law, the personal data controller must, prior to introducing biometric measures, supply the Information Commissioner with a description of intended measures and the reasons for this. The personal data controller must not start implementing biometric measures without prior decision of the Information Commissioner. The Information Commissioner is obliged to bring a decision within two months whether the measures comply with the provisions of ZVOP-1. The deadline may be extended by a maximum of one month if the introduction of such measures would affect more than 20 employees in a person in the private sector, or if the trade union representative requires the employer to participate in the administrative procedure. No appeal is possible against the decision of the Information Commissioner, but an administrative dispute is permitted.

Biometric measures in the public sector can be introduced in connection with entry into a building or parts of the building and recording the presence of employees at work. Prior to this, the public sector representative must obtain a positive decision from the Information. From the viewpoint of the proportionality principle, the Commissioner must find out whether applying biometric measures is really necessary for implementing the activities, for the safety of people or property, and for the protection of secret data or trade secrets.

4. Records of entry to and exit from premises

The provisions for entry to and exit from the premises are identical for both, the private and the public sector. For the purpose of protecting property, lives and health of individuals and keeping order in their premises, the individuals may be required to state some of their personal data and the reasons for entry or exit. If required, personal data can be verified by examining a personal document. The records for entry and exits about an individual may only contain the following personal data: personal name, number and type of personal document, address of permanent or temporary residence, employment, and date, time and reason for entry or exit to or from the premises. Personal data from such records can be stored for a maximum of three years from their recording, after which they must be erased, or otherwise destroyed.

5. Public books and linking of file systems

In questions of processing personal data obtained from public books, we need to take into account the legal purpose for which a public book was established. Personal data from a public book, regulated by the law, can be used only in ac-

cordance with the purpose for which they were collected and processed, and if the statutary purpose of their collection or processing is defined or definable.

Filing systems from official records and public books are allowed to be linked only if provided by the law. When linking two or more filing systems, which are kept for different purposes, the data controller is obliged to inform the Information Commissioner in writing.

A special protection is provided for filing systems, containing sensitive personal data, when linking would result in the disclosure of sensitive data, or if the implementation of linking would require the use of same connecting code. In such cases linking is not allowed without prior consent of the Information Commissioner.

The Information Commissioner can permit linking of filing systems based on a written application of the data controller, if it is ensured that adequate personal data protection is provided. There is no appeal against the decision of the Commissioner, but an administrative dispute is permitted.

It is always prohibited to link filing systems from criminal records and minor offence records with other filing systems and linking filing systems from criminal records and minor offence records.

ВОЛЬНЫЙ ОТДЫХ

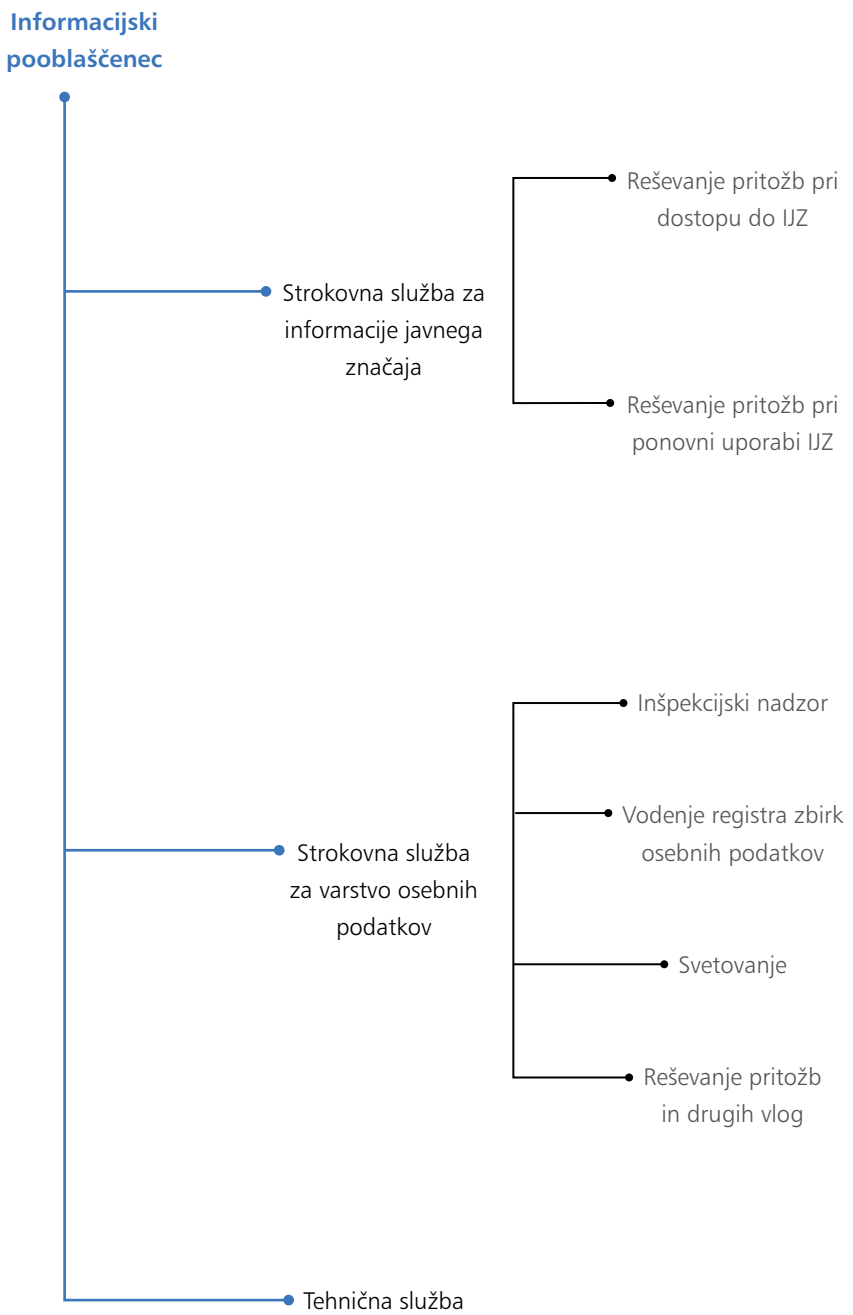

LIFE, too long to be negative
5

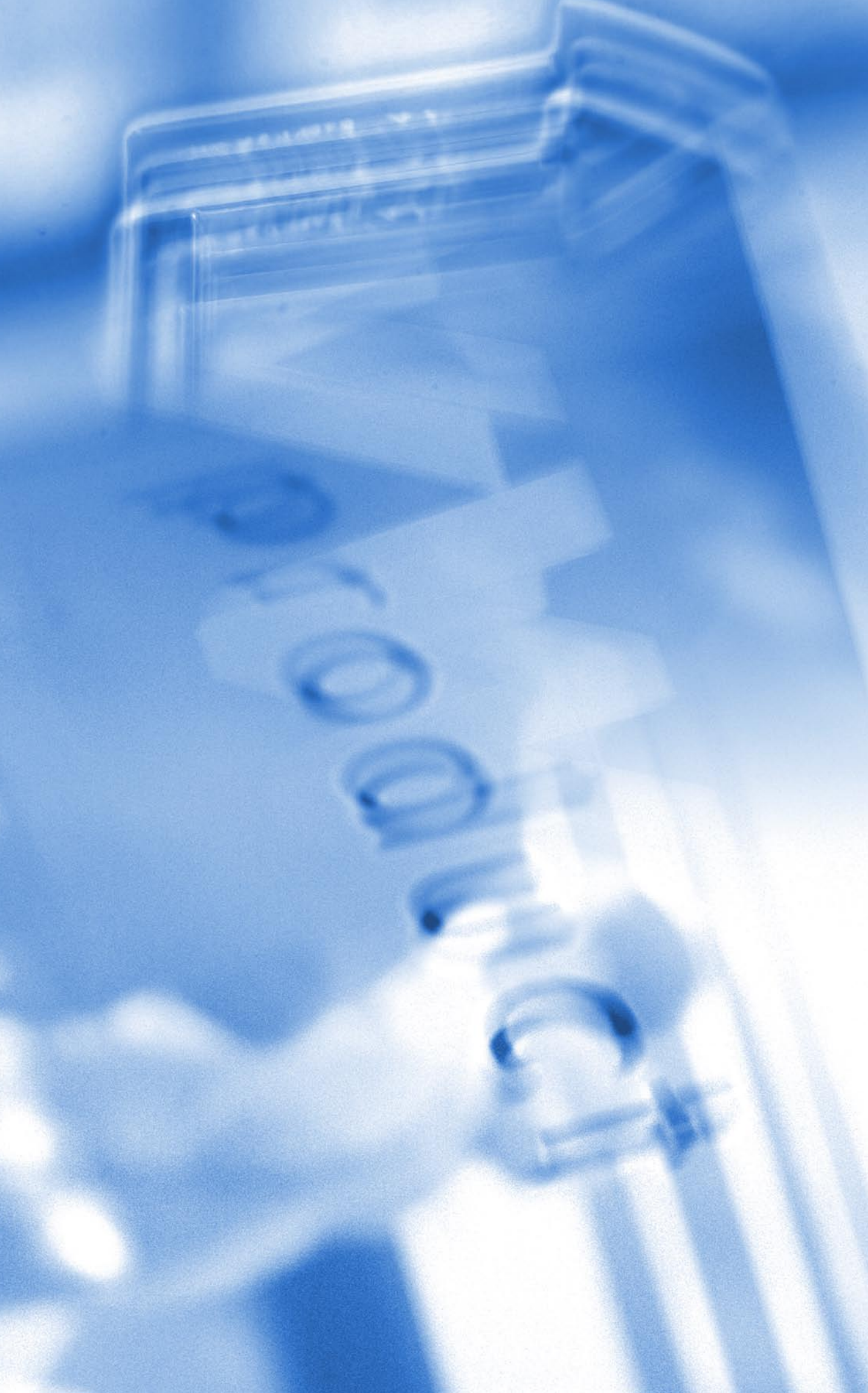
Nataša Pirc Musar was born in Ljubljana, in 1968. She graduated from the Faculty of Law in 1992, and took bar examination in 1997. After completing her studies she took a job at the national TV station, working as a journalist and leading the central information programme "TV Dnevnik". Later on, she got a position of the leader of the central news (information) programme "24 ur" at a commercial TV station, POP TV.

She upgraded her journalist experience working for CNN, Atlanta, U.S.A. Later on, she took a two-semester course at the Media Department of the University of Manchester, UK. Her studies included practical work at TV stations, e.g. BBC, Granada TV, Sky News, Reuter TV and Border TV. She published numerous articles in newspapers and appeared on various radio programmes. Driven by a desire to acquire new knowledge in a different setting, she took a job of the Head of Corporate Communication in the Aktiva Group Company in 2001, which is one of the leading private financial companies in Slovenia. On April 2003 she was offered a job at the Supreme Court of Slovenia, working as a manager of the Centre for Education and Information. On July 2004, on a proposal from the President of the Republic Slovenia, Dr. Janez Drnov'ek, she was appointed a Commissioner for Access to Public Information by the National Assembly, and since the Information Commissioner Act has adopted, she has been acting as the Information Commissioner.

6

Information Commissioner is an independent state body, established by the Information Commissioner Act, adopted on Dec 2005. This office replaced two previous bodies, i.e. the Commissioner for Access to Public Information and the Inspectorate for the protection of personal data. The main functions of the body are the protection of personal data and performing supervision over the transparency of the activities of other bodies of the public sector and ensuring that the work of the bodies is public and open. The following organigram shows the organisational structure:





INFORMACIJSKI
POOBLAŠČENEC

REPUBLIKA SLOVENIJA

INFORMATION COMMISSIONER

E-mail: gp.ip@ip-rs.si

Tax number: 89502868, IP is not taxable

Registration number: 1867571

Bank account: 01100-6300109972

http://www.ic-rs.si

Prepared by the Information Commissioner

Managing editor: Klemen Mišič

Authors: Nataša Pirc Musar
Mojca Prelesnik
Sonja Bien
Klemen Mišič

Translation: Nada Vukadinovič

Graphic design: Bons

Printed by: Premoere, d. o. o.

Print run: 500

Published by: Information Commissioner on March, 2006