

FRALEX

Thematic Legal Study on assessment of data protection measures and relevant institutions

Slovak Republic
Via Iuris and ETC
March 2009

DISCLAIMER: This thematic legal study was commissioned as background material for the comparative report on *Data protection in the European Union: the role of National Data Protection Authorities* by the European Union Agency for Fundamental Rights (FRA). It was prepared under contract by the FRA's research network FRALEX. The views expressed in this thematic legal study do not necessarily reflect the views or the official position of the FRA. This study is made publicly available for information purposes only and do not constitute legal advice or legal opinion.

1.	Overview.....	6
2.	Data Protection Authority.....	11
2.1	Powers of the Office for Personal Data Protection of the Slovak Republic	12
2.2	The Remit of the Office for Personal Data Protection of the Slovak Republic	15
2.3	The Guarantees of Effectiveness and Independence of the Office.....	17
2.4	Other Activities of the Office for Personal Data Protection of the Slovak Republic	18
3.	Compliance	22
3.1	Registration	22
3.1.1	Special Registration	24
3.2	Written record	24
3.3	Data protection officers	25
4.	Sanctions, Compensation and Legal Consequences	27
4.1	Order.....	27
4.2	Publishing the Information on Violation of the Act.....	28
4.3	Sanctions for Administrative Offences	28
4.4	Disciplinary Fines	29
4.5	Notification of the Authorities responsible for Criminal Proceedings	29
4.6	Follow up Activities of the Office for Personal Data Protection	29
4.7	Protection of Personal Data Processed in the Context of Employment	31
5.	Rights Awareness	33
6.	Analysis of Deficiencies	35
7.	Good Practice.....	37
	ANNEXES	38

Executive Summary

- [1]. The Slovak Republic is a party to all significant international agreements in the field of personal data protection. The Slovak Constitution guarantees the right to privacy, including the right to be protected against unjustified collection, disclosure and other misuse of person's data.
- [2]. The first law specialised on protection of personal data was adopted in the former Czecho-Slovak Federative Republic in 1992. This act was later abolished and the latest Act on Protection of Personal Data¹ was adopted in 2002. One of the amendments² to the Act transposed the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- [3]. A data protection authority - the Office for Personal Data Protection – was established by the Act on Protection of Personal Data. The Office is an independent state authority with supervisory powers over the protection of personal data. Its President is elected by the National Council of the Slovak Republic upon proposal of the government and is responsible to the National Council. A Vice-President and inspectors are appointed by the government upon proposal of the President.
- [4]. The powers of the Office stipulated by the law are expressing its role in the field of personal data protection: the Office continuously monitors the state of personal data protection and the registration of information systems; it issues recommendations and binding opinions to improve the quality of protection of personal data in their processing; the Office also deals with complaints of data subjects and other persons and executes inspections based on the complaints or on its own initiative; it imposes sanctions and other measures to remove deficiencies. The Office shall participate also in legislative procedures and in the preparation of legislative proposals in the field of personal data protection.
- [5]. The Office has made public its binding opinions and recommendations (through its official web page), however its decisions on violations of the law and decisions on sanctions are not available to the public at all (except of verdicts on the sanction such as fines, without information about the violator and without

¹ Slovakia/zákon 428/2002 (03.07.2002)

² Slovakia/zákon 90/2005 (03.02.2005)

providing grounds for the decisions). The official web page is considered to be one of the means of communication of the Office to the public.

- [6]. Before processing personal data the information systems shall be registered by the Office, or shall be registered in a special registration, or shall be listed in a written record kept by the controller. The registers must be updated by the controllers and the Office shall be notified of any changes which are made within the information system. In case of a special registration the Office shall assess whether processing of personal data is unlikely to affect adversely the rights and freedoms of data subjects; the decision shall be issued within 60 days.
- [7]. The controller is responsible for internal supervision of protection of personal data processed. If he/she employs more than five employees, a personal data protection official shall be authorised who shall undergo a special training on the content of the Act on Protection of Personal Data and on the obligations imposed by the law. The personal data protection officials shall supervise all activities regarding processing of personal data, provide communications to the Office, supervise the transborder personal data flow and keep written records on the information systems which are not subject to the registration.
- [8]. The Office for Personal Data Protection is empowered to the various measures and sanctions which are applied in case of violation of the Act. The Office can issue an Order, can decide that certain information about the violator shall be made public, can impose sanctions (fines) for administrative offences or can impose disciplinary fines (in case of improper cooperation with the Office, etc.). The Office shall initiate inspections and commence proceedings either upon its own motion or based on the complaints of data subjects or other persons.
- [9]. The information systems in the context of employment are regulated by the Act on Protection of Personal Data as well as by special laws regulating employment relationships. Albeit trade-unions protect interests of employees, they are not formally assigned to monitor compliance with the applicable legislation concerning protection of personal data.
- [10]. Public awareness concerning personal data protection is quite low in the Slovak Republic and this is only slowly changing. This can be proved by the surveys implemented in this field. Their outcomes are reflected in the report of the Office.

- [11]. The main deficiencies identified in the field of personal data protection are shortage in staffing and budget of the Office; unreasonable perplexity and complexity of the law which is quite confusing for regular users as well as for the controllers and processors; low public awareness of the law, its obligations and of the right to protect one's personal data.

1. Overview

- [12]. The protection of personal data belongs to the group of fundamental human rights and freedoms. Constitutional framework of data protection in the Slovak Republic is defined by Article 19 of the Constitution³ as follows: “Everyone shall have the right to maintain and protect his or her own dignity, honour, reputation and good name. Everyone shall have the right to be free from unjustified interference with his or her private and family life. Everyone shall have the right to be protected against unjustified collection, disclosure and other misuse of his or her personal data.”
- [13]. Data protection interferes also with the freedom of expression and the right to information. The Constitution guarantees freedom of expression and the right to seek and disseminate information but it also states that these rights may be restricted by law if it is necessary in a democratic society to protect the rights and freedoms of others, national security, public order, protection of public health and morals.⁴
- [14]. Based on the provisions cited it is clear that the right to information is guaranteed unless it is confronted with the data protection of a person. In such case the Constitution protects everybody from unjustified collection, publication and/or other misuse of information concerning personal data.
- [15]. International framework of data protection is set up by all main relevant documents: the EU Charter of Fundamental Rights (ratified by the Slovak Republic on 12 May 2008), the European Convention on Human Rights (ratified on 18 March 1992), the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ratified on 13 September 2000) and its Additional Protocol (ratified on 24 July 2002), the Convention on Human Rights and Biomedicine (ratified on 15 January 1998), the International Covenant on Civil and Political Rights which the Slovak Republic has acceded to on 1 January 1993 as one of the succession countries of the Czechoslovakia.
- [16]. The Slovak Republic has transposed Directive 2002/58/EC of 12 July 2002 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector by the Act on Electronic

³ Slovakia/Ústava 460/1992 (01.09.1992)

⁴ Article 26 paragraph 4 of the Constitution of the Slovak Republic.

Communications.⁵ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC was transposed by the amending law⁶ of the Act on Electronic Communications.

- [17]. Basic legislation relating to data protection in the Slovak Republic consists of the Freedom of Information Act⁷ and the Act on Protection of Personal Data⁸ which create the framework of the right to seek and receive information on one side and the right to privacy on the other one.
- [18]. The Freedom of Information Act was adopted in 2000. Information relating to personality and privacy of a natural person, as well as personal data of a natural person processed by information systems shall be provided upon request only if it is so stipulated in a special law or with a prior consent of the person affected. Should the affected person be dead, consent may be given by a close relative.⁹ The Freedom of Information Act specifies also exemptions from the restriction of access to information: Specific personal data concerning public officials shall be provided upon request, namely title, name and surname, function within the office and day of appointment into the office, professional position and the day of commencement of functioning, locality of the office, the relevant state authority, salary and other financial earnings provided for the performance of the function if covered by the public budget. In case of police officers such information can be provided upon request only if disclosure of information is not threatening public security or national defence, protection of public order or other mission fulfilment.¹⁰
- [19]. The first Slovak specialised law on data protection in information systems was adopted in 1992.¹¹ This law was replaced in 1998 by the Act on Protection of Personal Data in Information Systems.¹² Finally, a new Act on Protection of Personal Data¹³ was adopted in 2002 and this law transposed Directive 95/46/EC of the European Parliament

⁵ Slovakia/zákon 610/2003 (03.12.2003)

⁶ Slovakia/zákon 654/2007 (11.12.2007)

⁷ Slovakia/zákon 211/2000 (17.05.2000)

⁸ Slovakia/zákon 428/2002 (03.07.2002)

⁹ Article 9 paragraph 1 and 2, Slovakia/zákon 211/2000 (17.05.2000)

¹⁰ Article 9 paragraph 3 and 4, Slovakia/zákon 211/2000 (17.05.2000)

¹¹ Slovakia/zákon 256/1992 (29.04.1992)

¹² Slovakia/zákon 52/1998 (03.02.1998)

¹³ Slovakia/zákon 428/2002 (03.07.2002)

and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The law regulates personal data protection of natural persons, principles of personal data processing, security of processing, protection of the rights of data subjects, transborder personal data flow, registration and keeping of records of information systems, and founding, status and scope of powers of the Office of Personal Data Protection of the Slovak Republic.

- [20]. In case of unlawful use and/or processing of personal data individual persons can use measures and remedies determined by the Act on Data Protection (see further Chapter 4 of this study). Besides those measures there are other general remedies, such civil law defamation lawsuit. According to the Civil Code, “A natural person has the right to protect his/her personality, in particular his/her life and health, reputation and human dignity, as well as privacy, name and other expression of personal nature”.¹⁴ In civil proceedings such person individuals can demand that the defendant (violator) is obliged to refrain from unlawful interference with his/her privacy and personal life, to eliminate negative effects and to provide satisfaction and compensation.¹⁵
- [21]. The Slovak Republic lacks a national debate regarding the effectiveness of the data protection. In recent years the access to information has been widely debated and it is still in the centre of discussions within civil society. The right to seek and receive information is considered to be one of the most important constitutional rights in order to establish well functioning public control over the state and municipal administration. On the other side, the question of personal data protection is still unappreciated and not debated broadly. According to the Office for Personal Data Protection of the Slovak Republic there is no general public discussion concerning the effectiveness of the data protection.¹⁶
- [22]. Low awareness of data protection is confirmed also by the outcomes of the survey on information security in the Slovak Republic in 2008. This survey proves quite low knowledge concerning data protection among citizens. More than 50 % of the respondents are confident that information security in the Slovak Republic is better than in Western European countries and more than 80 % of the respondents consider information security within their organisations as good or very good. On the other side, more than one third of interviewed companies

¹⁴ Article 11 of the Civil Code, Slovakia/zákon 40/1964 (26.02.1964)

¹⁵ Article 13 of the Civil Code.

¹⁶ Written response of the Office for Personal Data Protection of the Slovak Republic to the information request submitted by the author of this study, 23.01.2008.

have no monitoring system for security incidents and more than half of them only monitor some of the security threats. Over half of the companies have no disaster recovery planning. The survey showed also great access of third persons to the internal networks of respondents (41 % suppliers or subjects providing support and maintenance, 24 % suppliers of outsourcing services, 13 % clients). The general outcome of the survey is that companies in general do not make investments into new IT solutions regarding data protection and they operate in existing, passive regimes.¹⁷

- [23]. The outcomes of two surveys realised by the Statistical Office of the Slovak Republic are presented at the official web page of the Office for Protection of Personal Data.¹⁸ Based on the findings of the later survey, 51 % of the respondents declared their awareness concerning the right to data protection, but less than 50 % of them recognised the Office for Personal Data Protection as a relevant authority. It is also clear that the respondents do not use their right properly, since 90 % of them have never asked for information concerning processing of their personal data and only five per cent of them asked for rectification of personal data.
- [24]. More vivid discussion concerning personal data protection has occurred in 2007 in relation to the draft law on electronic communication which was supposed to enable storing of data concerning phone calls, short messages, e-mail communication and access to such data without prior court approval. Other topics discussed were the establishing of the central medical documentation and releasing of personal identification numbers of natural persons on the internet version of the land register.¹⁹ There is only a few people actively discussing the topic of data protection²⁰ and besides the official web page of the Office of Personal Data Protection²¹ there is only one active public web page on personal data protection.²²
- [25]. Based on above mentioned unofficial information (cited web pages, blogs) the main deficiencies concerning data protection in Slovakia arise from low awareness of the public, lack of case law and

¹⁷ http://www.infoware.sk/buxus_dev/generate_page.php?page_id=58195 (26.01.2009)

¹⁸ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=421 (19.01.2009)

¹⁹ <http://vyskoc.blog.sme.sk/c/111489/Ochrana-sukromia-pohlad-na-posledne-mesiace.html> (23.01.2009)

²⁰ For example <http://vyskoc.blog.sme.sk/>, <http://www.blog.mico.sk/> or <http://stellahanzelova.blog.sme.sk>

²¹ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=92

²² <http://www.oou.sk/>

complicated and unclear wording of the legislation (e.g. negative description of the object of the Act).²³

²³ <http://vyskoc.blog.sme.sk/c/152939/Zodpoveda-nase-chapanie-sukromia-dnesnej-dobe.html>
(23.01.2009)

2. Data Protection Authority

- [26]. Úrad na ochranu osobných údajov [The Office for Personal Data Protection of the Slovak Republic] was established by the Act on Protection of Personal Data²⁴ and replaced the office of the Plenipotentiary of the Government for Personal Data Protection. The Office is based in Bratislava and has competence to operate nationwide.
- [27]. The Office is a budgetary organisation and its budget is a part of the budgetary chapter of the Governmental Office of the Slovak Republic. The budget of the Office for 2008 was 960 850 EUR and is slightly lower for 2009 – 945 828 EUR.²⁵ According to the statement of the President of the Office it is striving for its separate budgetary chapter.²⁶
- [28]. The Office is chaired by the President of the Office elected by the National Council of the Slovak Republic upon proposal of the Government of the Slovak Republic. The term of the Office is five years and the president can be re-elected for a maximum of two consecutive terms. The President must be a Slovak citizen, nonpartisan and unimpeachable with an academic degree and with at least ten years of professional experience in the field of information technology or law.²⁷ During absence of the President he/she is represented by the Vice-President of the Office. The Vice-President shall be appointed by the Government of the Slovak Republic upon proposal of the President of the Office.²⁸ The same process of appointing into the Office applies also to the inspectors. The inspectors shall execute inspection activities of the Office. They are subordinated to the Chief Inspector.²⁹
- [29]. Other details concerning organisation of the Office shall be regulated by the internal rules. The Office consists of four main sections: Section of personal data protection inspection (chaired by the Chief Inspector), Section of legal and foreign relations (chaired by the

²⁴ Article 33, Slovakia/zákon 428/2002 (03.07.2002)

²⁵ Written response of the Office for Personal Data Protection of the Slovak Republic to the information request submitted by the author of this study, 22.01.2008

²⁶ <http://www.sme.sk/c/3532660/Gyula-Veszelei-Nie-sme-nesvojpravni-aby-nam-niekto-daval-recepty.html> (22.01.2009)

²⁷ Article 35, Slovakia/zákon 428/2002 (03.07.2002)

²⁸ Article 36, Slovakia/zákon 428/2002 (03.07.2002)

²⁹ Article 37, Slovakia/zákon 428/2002 (03.07.2002)

Vice-President), Service Office (chaired by the Head of the Service office), and the President's Secretariat.

- [30]. Staff of the Office consists at present of 35 employees³⁰ which is 81 % of the total number of employees.³¹ Considering many various and comprehensive powers and duties of the Office (see further) and its territorial operation it is evident that the stuffing (and related finances) is insufficient to ensure effective use of the powers given to the Office.

2.1 Powers of the Office for Personal Data Protection of the Slovak Republic

- [31]. The powers of the data protection authority pursuant to Article 28 of the Directive 95/46/EC are transposed by the Act on Protection of Personal Data, in particular by its third part dealing with the data protection authority.³²
- [32]. The Office shall participate in the process of drafting generally binding regulations in the field of personal data protection³³ and shall provide opinions on draft laws and other generally binding regulations regulating processing of personal data.³⁴ The Office shall issue generally binding legal regulations within the scope of its powers.³⁵ If the Office determines facts indicating that a law, a generally binding regulation or an internal regulation issued by the controller violate the fundamental rights and freedoms of natural persons in the processing of their personal data, the President of the Office may file a petition to the respective authority to change or cancel the regulation.³⁶ However, according to the Constitution of the Slovak Republic, the Office is not listed among the authorities entitled to file a petition with the Constitutional Court to examine constitutionality of a law.³⁷ Such power could be useful in cases when a law is in conflict with the constitutional right to privacy.

³⁰ Written response of the Office for Personal Data Protection of the Slovak Republic to the information request submitted by the author of this study, 22.01.2008

³¹ Written response of the Office for Personal Data Protection of the Slovak Republic to the information request submitted by the author of this study, 23.01.2008

³² Slovakia/zákon 428/2002 (03.07.2002)

³³ Article 38 paragraph 1(l), Slovakia/zákon 428/2002 (03.07.2002)

³⁴ Article 38 paragraph 1(n), Slovakia/zákon 428/2002 (03.07.2002)

³⁵ Article 38 paragraph 1(m), Slovakia/zákon 428/2002 (03.07.2002)

³⁶ Article 38 paragraph 3, Slovakia/zákon 428/2002 (03.07.2002)

³⁷ Article 130, Slovakia/constitution 460/1992 (01.09.1992)

- [33]. The inspectors (responsible for inspection activities), the President and the Vice-President are entitled to supervise respect for obligations during processing of personal data. To carry out such powers the representatives of the Office are entitled to enter the lands, buildings or other facilities of the controller and the processor, require from them (including their employees) relevant documents, other papers, statements and information, data processed on storage media including technical data carriers, reports and source codes of programmes (provided they are owned by the inspected persons) and other materials necessary for the inspection. Inspecting authorities are also entitled to request complete and true information (oral and/or written), statements and explanations regarding inspected and related facts and identified deficiencies. The inspectors are entitled to access the filing systems as the system administrator to the extent necessary to execute inspection. The inspected persons must cooperate with the inspectors and their identity can be verified by the inspectors.³⁸ The controller and the processor shall provide the Office with all relevant data in a determined time limit. They are obliged to report to the Office to provide further explanations and they are also obliged to bear all actions of the Office in order to clarify all circumstances necessary for an objective assessment of an investigated case.³⁹
- [34]. To execute provisions of Article 28 para. 3 second point of the Directive, the Office is entitled to issue an interim measure before commencement of the processing of personal data or in the course of such processing to the extent necessary for achieving the purpose of investigation; such interim measures can reside in the obligation to act, to refrain from some activity or to bear some activity. In case of suspicion that a duty imposed by the Act on Protection of Personal Data was breached the controller or the processor can be required to immediately block personal data or to temporarily suspend the activity that could endanger the fulfilment of such duty. In case of violation of the obligations pursuant to the Act the inspecting persons are entitled to impose on the controller or the processor the obligation to take measures to remove the identified deficiencies and their causes. The Office is further entitled to impose obligations of elaborating or completing of the relevant documents or the Security Project in accordance with the Act, and to impose the obligation to adopt technical, organisational and personal measures adequate to the method of the processing. The Office is also empowered to prohibit processing of personal data if it is contravening the Act, to order the removal or liquidation of personal data provided that they are or were unlawfully processed and to impose on the controller an

³⁸ Article 39 paragraph 1, Slovakia/zákon 428/2002 (03.07.2002)

³⁹ Article 44 paragraphs 2 to 4, Slovakia/zákon 428/2002 (03.07.2002)

obligation to cancel a written authorisation or a written contract with the processor. All tasks must be executed within the determined time limit. The controller and the processor are obliged to follow the requirements of the inspectors and shall inform the Office about their fulfilment.⁴⁰

- [35]. The transposition of the provision of Article 28 para. 3 third point of the Directive is incomplete. The Office has the power to investigate, inspect and deal with breaches of the Act on Protection of Personal Data, and such investigation can be initiated by notifications and petitions of legal and natural persons concerning suspicion of breaches of the obligations stipulated by the Act. The Office is also entitled to commence an investigation upon its own initiative.⁴¹ However, the Office is not entitled to initiate judicial procedures at the court. The access to court is guaranteed to all parties of proceedings in case of judicial review of the measures executed by the Office.⁴²
- [36]. Natural persons or legal entities may file a notification to the Office regarding a suspicion of a breach of the obligations or conditions stipulated by the Act on Protection of Personal Data. Such notification must be written and can be submitted by a data subject (i.e. a natural person whose personal data are processed) or any other natural person claiming that his/her rights stipulated by the Act are directly infringed.⁴³ The Office shall investigate and deal with the notification within time limit of 60 days and it shall inform the claimant about the outcome of the investigation. The information of the Office shall be written and shall highlight which rights of the claimant were breached. In case the Office does not reveal any violation of the Act it shall inform the claimant about this fact.⁴⁴ Notifications submitted by a natural person or a legal entity other than the claimant are disposed as if the proceedings were commenced by the Office upon its own initiative. Upon the request of such person the Office shall confirm the receipt of the notification; however, such person is not notified on the outcome of the investigation and is not considered to be a party of the proceedings.⁴⁵
- [37]. Based on the above mentioned findings there are two main deficiencies identified in the national legislation on personal data protection: a) The Office is not entitled to bring violations of the

⁴⁰ Article 46 paragraphs 1 and 2, Slovakia/zákon 428/2002 (03.07.2002)

⁴¹ Article 38 paragraph 1(f), article 45, Slovakia/zákon 428/2002 (03.07.2002)

⁴² Article 47, Slovakia/zákon 428/2002 (03.07.2002)

⁴³ Article 20 paragraph 6, article 45 paragraphs 1 and 2, Slovakia/zákon 428/2002 (03.07.2002)

⁴⁴ Article 45 paragraphs 12 and 13, Slovakia/zákon 428/2002 (03.07.2002)

⁴⁵ Article 45 paragraph 17, Slovakia/zákon 428/2002 (03.07.2002)

national provisions adopted pursuant to the Directive to the attention of the judicial authorities (Article 28 paragraph 3 third point), b) Pursuant to the national legislation the Office is not obliged to provide information on the outcome of the investigation to a person claiming for checks on the lawfulness of data processing. Based on the national law the Office is not obliged to inform other persons than a data subject or a natural person claiming that his/her rights stipulated by the Act were directly infringed – there are no rights guaranteed for the notification of associations or other legal entities.

- [38]. Other powers of the Office imposed by the Act on Protection of Personal Data are transposing the powers stipulated by Article 28 of the Directive. The Office is obliged to issue a report on the state of the protection of personal data at least once in two years.⁴⁶ After the report is discussed by the National Council of the Slovak Republic it shall be made public on the web page of the Office.⁴⁷ The Act applies to personal data processed despite the fact that the registered seat of a legal entity or the permanent residence of a natural person is not on the territory of the Slovak Republic.⁴⁸ In executing its supervising authorities the Office shall cooperate with similar data protection authorities executing their powers abroad.⁴⁹ All employees and staff of the Office (even after the termination of their employment) are subject to a duty of professional secrecy with regard to confidential information to which they have (had) access.

2.2 The Remit of the Office for Personal Data Protection of the Slovak Republic

- [39]. The Office shall execute independent supervision of the protection of personal data and participate in the protection of fundamental rights and freedoms of natural persons in the processing of their personal data. The Office shall not execute its supervision regarding personal data processed by information services – those are supervised by the National Council of the Slovak Republic.
- [40]. The Office shall fulfill the whole set of tasks stipulated by the Act on Protection of Personal Data:
- to inspect continuously the state of the personal data protection, registration and keeping of records by information systems;

⁴⁶ Article 38 paragraph 1(o), Slovakia/zákon 428/2002 (03.07.2002)

⁴⁷ Article 51 paragraph 3, Slovakia/zákon 428/2002 (03.07.2002)

⁴⁸ Article 1 paragraphs 3 and 4, Slovakia/zákon 428/2002 (03.07.2002)

⁴⁹ Article 33 paragraph 6, Slovakia/zákon 428/2002 (03.07.2002)

- to issue recommendations for the controllers with measures for ensuring protection of personal data in the information systems;
- to issue binding opinions in case of doubts concerning the transboundary personal data flow, registration of information systems and concerning the fact whether the extent, contents and the manner of processing and use of the processed personal data is adequate to the purpose of their processing. Binding opinions must be implemented by the relevant subjects;
- to investigate cases upon notification or on its own initiative and to issue measures for removing the deficiencies ascertained during investigation;
- to summon the controller or the processor for explanation in case of suspicion that their legal obligations were breached;
- to inspect the processing of personal data in information systems;
- to impose sanctions in case of breaches of the law;
- to submit a petition to the authorities responsible for criminal proceedings in case of suspicion of a crime;
- to register the information systems and to provide access to the registration;
- to participate in the legislative process and to provide opinions on draft laws concerning legislation in the field of the personal data protection;
- to issue generally binding legal regulations within the scope of its powers;
- to submit reports to the National Council of the Slovak Republic on the state of the protection of personal data on a regular basis.⁵⁰

[41]. The President of the Office is entitled to file a petition with the respective authority for amendment or cancellation of any legal regulation if such regulation violates fundamental rights and freedoms of natural persons in the processing of their personal data. However, the President is not among the subjects competent to file a petition with the Constitutional Court of the Slovak Republic to demur at the constitutionality of such legislation. Neither can the Office initiate a judicial review in case of a breach of the right to protection of personal data.

⁵⁰ Article 38 paragraph 1, Slovakia/zákon 428/2002 (03.07.2002)

2.3 The Guarantees of Effectiveness and Independence of the Office

- [42]. The Act on Protection of Personal Data guarantees the independence of the Office as follows: “The Office, as a state authority, shall execute supervision of personal data protection independently and it shall participate in protection of the fundamental rights and freedoms of natural persons in the processing of personal data.”⁵¹ The Office has competence to execute its powers over the entire territory of the Slovak Republic.
- [43]. The independency of the Office is guaranteed also by other facts. The President of the Office is elected by the National Council of the Slovak Republic (Parliament) upon proposal of the Government of the Slovak Republic for the term of five years. The president can be disengaged from the function before the termination of his/her office only by the National Council of the Slovak Republic and based on the reasons stipulated by the Act on Protection of Personal Data: His/her health conditions have not allowed him/her to fulfil the obligations stipulated by the Act on a long-term basis, at least for one year; or he/she breached the obligation to fulfil the duty of professional secrecy. As mentioned above, the term of office of the President shall last for five years unlike the term of the members of the National Council of the Slovak Republic (their term lasts for four years). Moreover, the President can be re-elected for maximum one more term (all together two consecutive terms).⁵²
- [44]. The President may not be a member of a political party or movement and during performance of the function the President may not undertake his/her business or other profit-making activities. The President of the Office is liable for his/her activities only to the National Council of the Slovak Republic.⁵³ There is no other state authority executing powers over the Office.
- [45]. The Vice-President and the inspectors are appointed by the Government upon the proposal of the President of the Office.⁵⁴ This procedure guarantees that the President cannot misuse his/her authority when administrating the Office.
- [46]. The main concerns about independence of the Office may arise from the insufficient budget (the Office does not have its own budgetary

⁵¹ Article 33 paragraph 2, Slovakia/zákon 428/2002 (03.07.2002)

⁵² Article 35 paragraphs 2 and 13, Slovakia/zákon 428/2002 (03.07.2002)

⁵³ Article 35, paragraphs 5, 7 and 13, Slovakia/zákon 428/2002 (03.07.2002)

⁵⁴ Article 36 paragraph 3, article 37 paragraph 3, Slovakia/zákon 428/2002 (03.07.2002)

chapter) which is created by the Government and approved by the National Council of the Slovak Republic. Material deficiency may result in insufficient executing of powers and remit of the Office.

2.4 Other Activities of the Office for Personal Data Protection of the Slovak Republic

- [47]. The Office shall act on its own initiative or upon the notification of natural persons or legal entities. The inspectors shall inspect the state of the protection of personal data. Based on the findings of inspection the Office is entitled to issue recommendations for the controllers, binding opinions and remedial measures; it can also summon the controller or the processor to provide further explanation; in case of breaching the law the Office can propose sanctions. Any remit of the Office stipulated by the Act can be executed upon notification or upon the Office's own initiative, the Act on Protection of Personal Data does not distinguish between acting upon notification of a data subject or of third persons and acting commenced upon its own initiative.
- [48]. The Office can detect violations of data protection legislation in two ways: Based on its own inspection activities which commence upon its own initiative (the Office shall inspect continuously the state of protection of personal data, registration and records of information systems),⁵⁵ or based on the notification of third persons. The Act uses term "to inspect continuously the state of protection of personal data"; however there is no further explanation of such activity. There are no comprehensive data on inspections of the Office initiated on its own initiative. As stated above the staffing of the Office is not sufficient therefore the Office is barely capable to handle complaints, submissions and queries of natural and legal persons. The Office's activities initiated upon its own motion reflect the actual needs: in the first years of new legislation (especially in 2002-2003) the Office monitored correctness of the data protection registrations. Later its activities are mostly nationwide and dealing with selected problems, such as monitoring camera systems, the obligation to submit personal identity papers when entering some institutions, etc.
- [49]. All of the violations are detected within the formalised procedure of the inspectors. During the inspection proceedings the inspectors are entitled to enter the property of the inspected subjects, require access to all relevant documents and papers, processed information and registry. The inspectors are also qualified to require complex and

⁵⁵ Article 38 paragraph 1(a), Slovakia/zákon 428/2002 (03.07.2002)

true information from the inspected subjects and demand cooperation from them. All those activities are executed regardless the fact that the inspection was initiated by notification of the data subject or another natural or legal person, or on the own initiative of the Office. If any infringement of the Act on Protection of Personal Data is detected the inspector can impose measures and/or sanctions pursuant to the Act.⁵⁶ Once the Office commences the formalised procedure, it continues with it until the relevant verdict, regardless of the initiator of the proceedings. There are no differences between the proceedings initiated by a complaint or upon own initiative of the Office.

[50]. The Act on Protection of Personal Data does not regulate the obligation of the Office to make its decisions and/or opinions public. Some of the materials are published on the official web page of the Office⁵⁷ but those are random documents. There are only three binding opinions made public by the Office:⁵⁸

- Binding Opinion 1/2005 of 1 May 2005 concerning processing of personal data in library filing system,
- Binding Opinion 1/2004 of 12 May 2004 concerning processing of personal data in bank information systems regarding education, military service and housing,
- Binding Opinion 1/2003 of 10 January 2003 concerning processing of personal data by the Slovak Apothecary Chamber.⁵⁹

[51]. There are only two recommendations issued by the Office published on the web page of the Office:⁶⁰

- Recommendation to processing of property tax return of the employees of state services of 9 September 2002,
- Recommendation to using of monitoring cameras of 12 March 2001.⁶¹

[52]. The decisions issued by the Office⁶² are not available to the public at all. The Office refused to disclose its decisions⁶³ upon request of the author of this study, with regard to the Freedom of Information Act

⁵⁶ Article 39 and article 46, Slovakia/zákon 428/2002 (03.07.2002)

⁵⁷ <http://www.dataprotection.gov.sk> or www.uouu.sk

⁵⁸ Issued pursuant to the Article 38 paragraph 1(c), Slovakia/zákon 428/2002 (03.07.2002)

⁵⁹ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=126 (23.01.2009)

⁶⁰ Issued pursuant to the Article 38 paragraph 1(b), Slovakia/zákon 428/2002 (03.07.2002)

⁶¹ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=127 (23.01.2009)

⁶² Decisions issued pursuant to the Article 46, Slovakia/zákon 428/2002 (03.07.2002)

⁶³ Written decision of the Office on Protection of personal Data of the Slovak Republic concerning non-revealing of requested information (22.01.2009)

(FOIA).⁶⁴ The decision refers to the provision pursuant to which requested information shall not be disclosed if it concerns execution of inspection, monitoring or supervision by a public administration authority with the exception of information on decision.⁶⁵ However, this opinion of the Office was not reviewed by judicial authorities and there is no case law regarding disclosure of decisions of the Office for Personal Data Protection of the Slovak Republic.

- [53]. On the other side, in case of a breach of the obligations stipulated by the Act on Protection of Personal Data the Office can decide that the relevant decision, consisting of the verdict and the grounds of the decision shall be made public. Such information shall also include the name, registered office or permanent residence, and identification number of the subject that committed the illegal action. Moreover, the Office can impose on the controller or processor that characteristics of the facts of the case concerning the breach of protection of personal data shall be published in the mass media.⁶⁶ There is only one case of such sanction on the official web page of the Office – law violation by the Geodesy, Cartography and Cadastre Authority of the Slovak Republic.⁶⁷
- [54]. The Opinions of the Working Party established under Article 29 of Directive 95/46/EC are not considered binding and the Act on Protection of Personal Data does not stipulate any such obligation for the Office for Personal Data Protection. The Opinions might only represent a source of inspiration for the interpretation of data protection legislation through the acting of a representative of the Office for Protection of Personal Data of the Slovak Republic within the Working Party. According to the Reports of the Office meetings of the Working Party were source of inspiration concerning data protection in reservation systems of airline companies, or in relation to using public cameras systems or biometric data in travel documents.⁶⁸ A representative of the Slovak Republic within the Working Group was member of the sub-group for Internet.⁶⁹ There is no other evidence about any case where the opinions of the Working Party can be seen as having been inspirational for the Office.
- [55]. The Office shall participate in drafting new legislation concerning personal data protection and provide opinions on draft laws and other

⁶⁴ Slovakia/zákon 211/2000 (17.05.2000)

⁶⁵ Article 11 paragraph 1(g), Slovakia/zákon 211/2000 (17.05.2000)

⁶⁶ Article 48, Slovakia/zákon 428/2002 (03.07.2002)

⁶⁷ <http://www.dataprotection.gov.sk/buxus/docs/07092007.pdf> (23.01.2009)

⁶⁸ http://www.dataprotection.gov.sk/buxus/docs/sprava_o_stave_ooou_2004.pdf

⁶⁹ <http://www.dataprotection.gov.sk/buxus/docs/31082007.pdf>

generally binding legal regulations.⁷⁰ Those tasks of the Office are executed in accord with the Plan of Legislative Tasks of the Government of the Slovak Republic issued for each particular year. If such legal regulation is not prepared primarily by the Office, then the Office participates in commenting and consulting of such legislation. In 2008 the Office participated in legislation procedures of 328 draft regulations and provided 27 fundamental comments.⁷¹

- [56]. The awareness raising role of the Office is not formally encompassed in the relevant legislation, but the Office considers it to be important and significant.⁷² It is mostly executed by the official web page of the Office.⁷³ Based on the written statement of the Office it is one of the main tools used to increase public awareness concerning personal data protection.⁷⁴ There is some basic information concerning the Office, its structure, the President, tasks, powers and remits.⁷⁵ There is also structured information regarding registration of information systems and keeping records of them, responsible persons and basic legislation regarding data protection. Among other documents there are some European Union materials concerning data protection, Guidelines for the controller in case of transboundary transfer of personal data and press releases of the Office (the most recent one from the year 2007).⁷⁶ There are also reports of the Office issued in accordance with the Act on Protection of Personal Data.⁷⁷
- [57]. According to the written statement of the Office its representatives participate also in public media discussions and provide lectures on the protection of personal data.⁷⁸

⁷⁰ Article 38 paragraph 1(l), (n), Slovakia/zákon 211/2000 (17.05.2000)

⁷¹ Written decision of the Office on Protection of personal Data of the Slovak Republic concerning non-revealing of requested information (22.01.2009)

⁷² Written decision of the Office on Protection of personal Data of the Slovak Republic concerning non-revealing of requested information (22.01.2009)

⁷³ <http://www.dataprotection.gov.sk> and <http://www.uoou.sk>

⁷⁴ Written decision of the Office on Protection of personal Data of the Slovak Republic concerning non-revealing of requested information (22.01.2009)

⁷⁵ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=304,
http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=117 (23.01.2009)

⁷⁶ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=92 (22.01.2009)

⁷⁷ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=113 (22.01.2009)

⁷⁸ Written decision of the Office on Protection of personal Data of the Slovak Republic concerning non-revealing of requested information (22.01.2009)

3. Compliance

- [58]. The controllers are obliged to notify the supervisory data protection authority before carrying out automatic processing operation and to apply for registration of information system, or have to keep written record of information systems which are not subject to registration.

3.1 Registration

- [59]. The obligation to register shall apply to all information systems with wholly or partly automatic processing operation. There are following exemptions from the obligation to register:

- where the information system is subject to a special registration;
- where the controller appoints in written a personal data protection official;
- where the information system contains data on natural persons processed for the purposes of pre-contractual relations or for the purposes of exercising rights and obligations in the field of employment law, including data on close relatives of the natural persons concerned;
- where processing relates to the personal data of members of trade-union organisations and the data are used solely for the internal needs of the trade-union; the same applies to the members of officially recognised religious associations, and to the members of political parties or movements;
- where the information system contains data necessary for exercising the rights or fulfilment of the obligations arising from a special act; such special act is not identified in the Act on Protection of Personal Data.⁷⁹

- [60]. In case of doubts whether the information system is subject to registration, a decision shall be made by the Office for Personal Data Protection.⁸⁰ Unlike the directive, the Slovak legislation does not stipulate that the exemption from notification the supervisory data protection authority can be used only if it is unlikely that the processed personal data may affect adversely the rights and freedoms of data subjects. This deficiency can be significant especially in the case of the last exemption mentioned above – where the Act on Protection of Personal Data refers to an unspecified “special act”.

⁷⁹ Article 25 paragraph 2, Slovakia/zákon 428/2002 (03.07.2002)

⁸⁰ Article 25 paragraph 4, Slovakia/zákon 428/2002 (03.07.2002)

[61]. Information provided for the registration is as follows:

- the name, address, corporate form and identification number of the controller, or of his representative provided that he acts on the territory of the Slovak Republic on behalf of the controller who has his registered office or permanent residence in a third country;
- the name of the representative of the controller;
- the name of the personal data protection official;
- the identifier of the information system;
- the purpose of the processing;
- a list of personal data processed;
- a category of data subjects;
- the recipients and the third parties, provided that the data might be disclosed to them;
- third countries, provided that the data might be transferred to these countries, and a legal basis for such transborder flow;
- the legal basis for the information system;
- the form of publication, provided that personal data are to be made public;
- general characteristics of the measures for ensuring protection of personal data;
- the date of commencement of the processing of personal data.⁸¹

[62]. The controller shall notify the Office in writing within 15 days of any changes of the information provided for registration. The same applies to cancelling of the registration.⁸² Registration is free of charge.⁸³

[63]. The official web page of the Office for Personal Data Protection contains information on registration procedure, example of forms,⁸⁴ registers accessible for the public (providing that the public knows the name of the controller or his/her registration number) and abolished registration.⁸⁵ It is impossible to provide evidence regarding compliance with these duties in practice because the Office does not register proper data for such assessment.

⁸¹ Article 26 paragraph 3, Slovakia/zákon 428/2002 (03.07.2002)

⁸² Article 28 paragraphs 1 and 2, Slovakia/zákon 428/2002 (03.07.2002)

⁸³ Article 25 paragraph 1, Slovakia/zákon 428/2002 (03.07.2002)

⁸⁴ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=558 (23.01.2009)

⁸⁵ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=129 (23.01.2009)

3.1.1 Special Registration

- [64]. Special registration applies to information systems, which process:
- special categories of personal data, provided that their transfer to a third country not ensuring an adequate level of protection is expected;
 - personal data necessary for the protection of rights and legitimate interests of the controller or a third party, provided that fundamental rights and freedoms of a data subject are respected and are not illegally violated;
 - biometric data, except for analysis of DNA and DNA profile of natural persons for the purpose of registration or identification when entering sensitive, specially protected facilities or accessing technical mechanisms or devices with a high rate of risk, and such data are used solely for internal needs of the controller.⁸⁶
- [65]. The controller provides the Office with the same information as in case of registration of information systems. Providing that the Office considers the information system submitted for a special registration to be risky, it shall prohibit the processing of personal data for the respective purpose.⁸⁷
- [66]. The Office shall assess provided information, in particular whether processing of personal data is unlikely to affect adversely the rights and freedoms of data subjects. It shall decide on approval of special registration of an information system within 60 days. In case of doubts the Office can require additional information from the controller and postpone the deadline for issuing a decision.⁸⁸ It is impossible to provide evidence regarding compliance with these duties in practice because the Office does not register proper data for such assessment.

3.2 Written record

- [67]. Information systems which are not subject to registration are listed in a written record of the controller, at the latest from the day of commencement of processing such personal data. Pursuant to the Act on Protection of Personal Data the information systems are not even listed in a written record of the controller if:

⁸⁶ Article 27 paragraph 2, Slovakia/zákon 428/2002 (03.07.2002)

⁸⁷ Article 27 paragraph 9, Slovakia/zákon 428/2002 (03.07.2002)

⁸⁸ Article 27 paragraphs 5 and 6, Slovakia/zákon 428/2002 (03.07.2002)

- the processed personal data are solely for the needs of postal services with data subjects ;
- the sole purpose of processing personal data is identification or persons at their single entering of the controller's facilities.⁸⁹

[68]. Written records shall be made public upon request.⁹⁰

3.3 Data protection officers

[69]. The controller is responsible for internal supervision of protection of personal data processed pursuant to the Act on Protection of Personal Data. If the controller employs more than five employees he/she shall authorise one or more personal data protection officials. A data protection official shall complete training on the content and duties pursuant to the Act and on international standards concerning personal data protection. An evidence of such training shall be provided to the Office upon request. The Office shall be notified about the appointment of a data protection official without undue delay (at the latest within 30 days). The information provided to the Office are as follows:

- the name, registered office or permanent residence, corporate form and identification number of the controller (or his/her representative);
- the title, name, date of birth and working position of the data protection official;
- the date of effectiveness of the written authorisation;
- the controller's declaration stating that the personal data official fulfils all the requirements stipulated by the Act.⁹¹

[70]. A data protection official shall be a natural person, unimpeachable (i.e. not convicted of an intentional crime or not condemned to an unconditioned imprisonment). An official representative of the controller may not be appointed as data protection official.⁹²

[71]. Before commencement of the processing of personal data the personal data protection official shall assess whether processing is not likely to affect adversely fundamental rights and freedoms of data subjects. Any violation of rights and freedoms by processing of

⁸⁹ Article 29, Slovakia/zákon 428/2002 (03.07.2002)

⁹⁰ Article 32, Slovakia/zákon 428/2002 (03.07.2002)

⁹¹ Article 19 paragraph 5, Slovakia/zákon 428/2002 (03.07.2002)

⁹² Article 19 paragraph 12, Slovakia/zákon 428/2002 (03.07.2002)

personal data shall be reported to the controller with undue delay. If the controller does not rectify the situation, the personal data protection official shall notify the Office for Personal Data Protection. The data protection official shall supervise all activities regarding processing of personal data, provide communication to the Office, supervise the selection of the processor, supervise the transborder personal data flow, submit information systems to a special registration and notify the Office of any changes within the registered systems. He/she shall also keep written records on the information systems which are not subject to obligatory registration and shall make them available upon request.⁹³

- [72]. The personal data protection official is entitled to execute independent supervision over the protection of personal data. He/she can submit proposals, notifications concerning deficiencies or requests to the controller. If the official fails to fulfil sufficiently his/her duties pursuant to the Act on Protection of Personal Data, the Office is entitled to order the controller to authorise another person for the position of the personal data protection official.⁹⁴ It is impossible to provide evidence regarding compliance with these duties in practice because the Office does not register proper data for such assessment.

⁹³ Article 19 paragraphs 4 and 7, Slovakia/zákon 428/2002 (03.07.2002)

⁹⁴ Article 19 paragraphs 10 and 11, Slovakia/zákon 428/2002 (03.07.2002)

4. Sanctions, Compensation and Legal Consequences

- [73]. The Office for Personal Data Protection is empowered to use various means of sanctions and measures in case of violations of obligations stipulated by the Act on Protection of Personal Data. There is no reference concerning cases where the Office had notified the authorities responsible for criminal proceedings.
- [74]. The Act on Protection of Personal Data does not contain any provision concerning proving intent or negligence in proceedings. Legal measures are imposed in case the law was violated. However, pursuant to information from the Office the fines are imposed in cases of intentional responsibility. This practice is not reflecting legislation.

4.1 Order

- [75]. If the controller or the processor violate some of their obligations the Office can impose an order to:
- take measures to eliminate detected deficiencies and their causes;
 - elaborate or complete documentations or security projects pursuant to the Act on Protection of Personal Data;
 - take technical, organisational and personal measures adequate to the manner of the processing of data;
 - prohibit processing of the personal data, the processing of which is contrary to the provisions of the Act;
 - prohibit processing which is contrary to the provisions of the Act;
 - remove or destruct personal data which were processed illegitimately;
 - cancel written authorisation or written contracts with the processor.⁹⁵
- [76]. The controller and/or processor can submit objections; otherwise they have to implement the duties imposed by an order. Objections

⁹⁵ Article 46 paragraph 1, Slovakia/zákon 428/2002 (03.07.2002)

are reviewed by the President of the Office. The final decision is subject to judicial review.⁹⁶

- [77]. The Office may also impose temporary orders to take, refrain or bear some action or it can request the controller or the processor to immediately block personal data or to temporarily suspend the activity that could endanger the fulfilment of legal obligations.

4.2 Publishing the Information on Violation of the Act

- [78]. Another form of legal consequences of violations of the Act on Protection of Personal Data is publishing formal information on violations of the Act. If the provisions of the Act are violated or circumvented the President of the Office or the Chief Inspector may make public the following information of the violator:

- name, registered office, identification number and the corporate form of the person who committed the illegal action, and
- the verdict and the grounds of the order or of the decision on administrative sanction (except for personal data),
- characteristics of the factual state concerning the breach of protection of personal data.⁹⁷

- [79]. The President of the Office or the Chief Inspector can also impose on the controller or the processor an obligation to publish the above mentioned information in the mass media.

4.3 Sanctions for Administrative Offences

- [80]. The Office can impose a fine in the amount from 332 EUR up to 331.939 EUR, or in case of minor offences up to 3.319 EUR. The fine can be imposed repeatedly if the obligation was not fulfilled in time. The controller or the processor can appeal against the decision on the fine which is decided by the President of the Office.⁹⁸

⁹⁶ Article 46 paragraphs 3 to 6, Slovakia/zákon 428/2002 (03.07.2002)

⁹⁷ Article 48 paragraph 1, Slovakia/zákon 428/2002 (03.07.2002)

⁹⁸ Article 49, Slovakia/zákon 428/2002 (03.07.2002)

4.4 Disciplinary Fines

- [81]. The Office can impose a disciplinary fine if the controller or the processor fail to provide adequate conditions for execution of the inspection (up to 1.660 EUR); if the controller or the processor cause obstruction during inspection (up to 16.597 EUR); if the controller or the processor fail to make public in the mass media a notice determined by the Office (up to 33.194 EUR); if the controller or the processor do not provide the Office with requested cooperation or ignore the order of the Office (up to 66.388 EUR). A disciplinary fine may be imposed within one year after the day when the obligation was breached.⁹⁹

4.5 Notification of the Authorities responsible for Criminal Proceedings

- [82]. If there is a suspicion that a crime was committed the Office can notify the authorities responsible for criminal proceedings. Further investigation is executed by these authorities pursuant to legislation regarding criminal law.

4.6 Follow up Activities of the Office for Personal Data Protection

- [83]. The Office can ascertain information on suspicion of violation of the law either through its own-motion activities or based on the notifications/complaints of other subjects. Natural persons or legal entities can submit a written notification to the Office concerning violation of the obligations stipulated by the Act on Protection of Personal Data. Such notification shall be formalised and shall contain all relevant data stipulated by the Act (name and address of the notifier, subject of notification, description of the rights violated, evidence to support these findings, relevant documents, etc.). A notification can be put away only in cases stipulated by law. Otherwise the Office is obliged to deal with and review such notifications and inform the notifier about the outcome.
- [84]. If a notification is submitted by a natural person or a legal entity other than a natural person directly affected on his/her rights, such notification is reviewed as an own-motion investigation of the

⁹⁹ Article 50, Slovakia/zákon 428/2002 (03.07.2002)

Office. Such person is not party of proceedings and is not informed about the outcome of the investigation.

- [85]. Besides complaints the Office can initiate inspections and proceedings on its own-motion initiative. The Act on Protection of Personal Data does not distinguish between inspection commenced by the Office or initiated by other persons. In any case, the Office can use all powers provided by law to properly investigate any suspicion concerning violations of the Act, such as entering the property and facility of the controller and/or processor, requesting information, explanation and relevant documents from them or requiring cooperation from inspected subjects. At the end the inspection authority shall elaborate a protocol on the execution of the inspection.¹⁰⁰ The protocol is the basic document for further proceedings of the Office.
- [86]. Own-motion investigations of the Office are originating either in a plan of control of the Office (inspired by problems identified by the media or by more complaints concerning a specific problem) or in complaints of individuals. Based on such information the Office initiates nationwide inspections oriented to one problem as well as special inspections oriented to a specific type of subjects, or individual inspections.
- [87]. Based on the results of the investigation the Office can initiate proceedings on imposing relevant measures – orders, publication of the information on violations of the Act, and/or sanctions for administrative offences. All these procedures are carried out regardless of the fact who was the original initiator of the inspection.
- [88]. Further proceedings of the Office depend on the character and significance of the identified problem. First of all the Office deals with problems through consultations and advices. If these steps are not successful and the problem is not solved, the Office imposes orders and/or financial sanctions. In case of serious violations of the Act on the Protection of Personal Data the Office imposes fines without imposing any previous, more moderate measures.
- [89]. If the investigation is initiated by a complaint of a natural person (data subject), such a person is not entitled to any specific legal or other assistance from the Office nor another state authority. The Office does not provide any legal aid or legal representation to such person. The Office is a state authority responsible for investigation of violations of the Act while the data subject is a party to the

¹⁰⁰ Article 39, Slovakia/zákon 428/2002 (03.07.2002)

proceedings; if the Office provided special assistance to the data subject, the principle of equality before the law would be breached.

- [90]. There is also no other state authority or non-governmental organisation dealing specifically with violations of the Act on Protection of Personal Data and providing legal or other assistance to data subjects. In case of judicial review of the Office's decision, each party of the proceedings bears its own expenses. However, the court can decide that a successful party can be awarded compensation for court fees and related expenses.

4.7 Protection of Personal Data Processed in the Context of Employment

- [91]. Pursuant to the Act on Protection of Personal Data it is forbidden to process personal data revealing inter alia trade-union membership.¹⁰¹ However, this restriction shall not apply if a data subject provides a written consent with processing of data, or if the processing is necessary for the purposes of fulfilment of obligations or exercising the legitimate rights of the controller responsible for data processing in the field of labour law and employment services.¹⁰² The information systems, which contain personal data of natural persons processed for the purposes of exercising the rights and obligations resulting for the controller from an existing or terminated employment relationship shall not be subject to registration.¹⁰³
- [92]. Legislation in the field of employment law contains some special provisions concerning protection of personal data. The Act on Employment Services¹⁰⁴ stipulates that subjects arranging employment are responsible for the protection of personal data. Information systems of job applicants include the name, personal identification number, nationality, permanent residence or temporary residence address, information on qualification of the applicant, information on previous employment, data on personal and family relationships related to the job arrangement and information on health (provided on voluntary base).¹⁰⁵ These personal data can be revealed to other subjects only with previous consent of the job applicant.

¹⁰¹ Article 8 paragraph 1, Slovakia/zákon 428/2002 (03.07.2002)

¹⁰² Article 9 paragraph 1(f), Slovakia/zákon 428/2002 (03.07.2002)

¹⁰³ Article 25 paragraph 2(c), Slovakia/zákon 428/2002 (03.07.2002)

¹⁰⁴ Slovakia/zákon 5/2004 (04.12.2003)

¹⁰⁵ Article 33, Slovakia/zákon 5/2004 (04.12.2003)

- [93]. Conditions of a job offer may not permit any restrictions and/or discrimination based on race, skin colour, gender, age, language, religion, health disability, political or other persuasion, trade-union membership, national or social origin, ethnicity, possession, lineage, marital and family status. An employer cannot require from a job candidate information concerning his/her nationality, race, ethnicity, political attitude, membership in trade-unions, religion, sexual orientation or other data not necessary for the respective job position. An employer is obliged to prove necessity of provided personal data upon request of a job candidate.¹⁰⁶ Similar restrictions are stipulated by Labour Code.¹⁰⁷
- [94]. Trade-unions (if established) protect interests of employees through so called collective negotiations concerning employment conditions. No legislation stipulates explicitly the entitlement of trade-unions to be active in monitoring compliance with the applicable legislation concerning protection of personal data. However, it is possible to promote such protection through collective negotiations with an employer.

¹⁰⁶ Article 62, Slovakia/zákon 5/2004 (04.12.2003)

¹⁰⁷ Slovakia/zákon 311/2001 (02.07.2001)

5. Rights Awareness

[95]. There are regular public surveys concerning the protection of personal data in the Slovak Republic. Their outcomes are reflected in the reports issued by the Office for Personal Data Protection. Two of the surveys (conducted in 2005¹⁰⁸ and 2007¹⁰⁹) are published on the web page of the Office.¹¹⁰

[96]. All public surveys were carried out by the Public Opinion Research Centre of the Statistical Office of the Slovak Republic upon request of the Office for Personal Data Protection. The surveys were general, not targeted to any special segments of the society and the following questions were surveyed:

- public awareness of personal data protection rights within information systems;
- sensibility of personal rights in terms of their possible misuse;
- public awareness of obligations of subjects processing personal data;
- experience of the public in relation to requesting information from subjects processing personal data;
- public attitude towards including biometric data into travelling documents;
- public trust to the controllers of information systems;
- public awareness concerning available legal measures for the protection of personal data;
- public awareness concerning transboundary transfer of personal data;
- misuse of personal data in internet communications;
- monitoring of internet communication as one of the tools to fight terrorism.¹¹¹

[97]. The surveys prove that public awareness regarding data protection law and rights is not very high and is slightly increasing. The last survey ascertained that 51 % of the respondents declared their understanding of personal data protection. However, almost 90 % of

¹⁰⁸ http://www.dataprotection.gov.sk/buxus/docs/sprava_5_2005_prieskum_vm1.pdf (23.01.2009)

¹⁰⁹ http://www.dataprotection.gov.sk/buxus/docs/zaverecna_sprava_07.pdf (23.01.2009)

¹¹⁰ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=421 (22.01.2009)

¹¹¹ http://www.dataprotection.gov.sk/buxus/docs/zaverecna_sprava_07.pdf (23.01.2009)

the respondents never requested any information from the controller processing their personal data. Only half of the respondents are aware of the Office as a responsible state authority for the issue. Here are some of the outcomes: According to the survey personal identification numbers, data on property and data on health are among the most sensitive data, on the other side half of the respondents approved using of biometric data in their travelling documents; over two fifth of the respondents feel concerns regarding possible misuse of personal data in internet communication; the same number of respondents upholds monitoring of internet and telephonic communication (even without judicial approval) in regard to fighting terrorism.

6. Analysis of Deficiencies

- [98]. The Act on Protection of Personal Data in principle transposed provisions of the Directive correctly. However, the main defect of the Act is its overall perplexity and complexity of relationships. Protection of personal data is one of the fundamental rights guaranteed also by the Constitution of the Slovak Republic, therefore the fundamental legislation regulating this issue should be generally comprehensible and unambiguous. The same applies not only to data subjects, but also to subjects processing personal data. The Act regulates general aspects of processing of personal data, however there are many exemptions from basic rules, which is confusing and not understandable.
- [99]. There is also an incorrect transposition of some provisions of the Directive: The Directive stipulates that Member States may provide for simplification of or exemption from notification only in explicitly stipulated cases which include the important condition, that the processed data are unlikely to affect adversely the rights and freedoms of data subjects.¹¹² Slovak legislation did not include such a condition in the exemptions from registration of the information systems. It might be important especially in cases of doubts whether a respective system should be registered or not.
- [100]. With regard to the number of subjects and the quantity of information systems processed, it is impossible for the Office to effectively execute its powers, especially concerning monitoring, inspecting and awareness raising tasks. Low budget and small staff of the Office do not allow executing all tasks adequately and sufficiently.
- [101]. General public awareness regarding protection of personal data is very low at present. The public does not attach importance to the topic and has very low acquaintance on the powers and remits of the Office for Personal Data Protection, in fact only half of the population has recognised the existence of the Office.
- [102]. The Act does not cover the protection of personal data which were acquired accidentally, without previous identification of the purpose or data processed by a natural person for his/her own needs within personal activities (such as correspondence, address book, etc).

¹¹² Article 18, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

- [103]. The above mentioned deficiencies might be reduced by amendment to the existing legislation to simplify existing legal regulation, so it is comprehensible for all related subjects. Another step should be increasing of resources of the Office for Personal Data Protection, namely concerning its staffing and budget. And finally, activities raising public awareness concerning protection of personal data are inevitable.

7. Good Practice

- [104]. The Office for Personal Data Protection issues regular reports which are available for the public through the official web page of the Office. These reports are quite comprehensive and include not only information about the activities of the Office, but also quite detailed description of relevant problems dealt with during the respective reported period. This approach is very useful for lay public, as well as for the controllers and processors. Such reports represent a great instrument for raising public awareness in the topic.

Annexes

Annex 1 – Tables and Statistics

[105]. The data cited in the following table are based on information included in reports of the Office for Personal Data Protection of the Slovak Republic¹¹³ and on written responses of the Office to the information request of the author of this study.¹¹⁴ Some of the data are not available for the whole calendar year, some of them are available for more than one year. There is no statistics concerning monitoring of the follow-up activities of the Office.

¹¹³ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=318 (23.01.2009)

¹¹⁴ Written responses of the Office of 22.01.2009 and 29.01.2009

	2000	2001	2002	2003	2004	2005	2006	2007	2008
Budget of the Office (in thousands of SKK) ¹¹⁵	7,709	7,134	9,110	20,778	23,264	21,532	23,500	26,285	28,946
Staff of the Office	12	11 ¹¹⁶	19	25	26	29	31	32	35
Number of procedures initiated by the Office at own initiative	150	data n.a. ¹¹⁷	14	data n.a.	data n.a.	121 ¹¹⁸			74
Number of data protection registrations	260	data n.a.	1,752 ¹¹⁹	3,321 ¹²⁰			6,300 ¹²¹		data n.a.
Number of data protection approval procedures	125	data n.a.	968	data n.a.	data n.a.	data n.a.	data n.a.	data n.a.	data n.a.
Number of complaints received by the	data n.a.	118	50	data n.a.	data n.a.	67	102	32 ¹²²	273

¹¹⁵ Conversion rate since 01.01.2009: 1 EUR = 30.126 SKK.

¹¹⁶ Out of eleven employees only eight were on full time positions.

¹¹⁷ Data n.a.=data not available.

¹¹⁸ Data available for time period 01.04.2005-31.03.2007.

¹¹⁹ Data available for time period 01.10.2001-31.03.2003

¹²⁰ Data available for time period 01.04.2003-31.03.2005.

¹²¹ Data available for time period 01.04.2003-31.03.2007.

¹²² Data available up to 31.03.2007.

Office									
Sanctions and/or compensation in data protection cases	data n.a ¹²³	data n.a	data n.a	1	0	0	1	7	14
Range of sanctions and/or compensation (in thousands of SKK) ¹²⁴	data n.a	data n.a	data n.a	200	0	0	10	3-40	10-250

Annex 2 – Case Law

[106]. The Office for Personal Data Protection of the Slovak Republic does not make public the decisions issued by the Office. The same applies to the judgements of the courts. Based on the written decision of the Office refusing disclosure of court rulings¹²⁵ such information is an exemption from the right to information guaranteed by the Constitution of the Slovak Republic and regulated by the Freedom of Information Act (FOIA).¹²⁶ Pursuant to FOIA requested information shall not be disclosed if it concerns execution of control, monitoring or supervision by a public administration authority with the exception of information on decision.¹²⁷ This opinion of the Office was not subject to judicial review and the author of this study presumes that the cited interpretation of the relevant provision of FOIA is not correct. This measure is not necessary in a democratic society to protect the rights and freedoms of others, safety of the state, public order, protection of public health or morality. As mentioned in Chapter 4.2 of this Study, one of the legal sanctions used in case of violation of the Act on Protection of Personal Data is

¹²³ The Office for Personal Data Protection of the Slovak Republic was created only by the Act 428/2002 (03.07.2002)

¹²⁴ Conversion rate since 01.01.2009: 1 EUR = 30.126 SKK.

¹²⁵ Written decision of the Office refusing disclosure of requested information (22.01.2009)

¹²⁶ Slovakia/zákon 211/2000 (17.05.2000)

¹²⁷ Article 11 paragraph 1(g), Slovakia/zákon 211/2000 (17.05.2000)

making public the decision on violation, including name and address of the violator. However, it is upon the Office to decide in which cases such sanction is appropriate.

- [107]. Some of the cases dealt with are discussed in the Reports of the Office which are publicly available at the official web page of the Office, but these Reports do not provide detailed and revealing information to be accurately distilled according to the established table format.¹²⁸

¹²⁸ http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=318 (23.01.2009),
Slovak version is available at:
http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=113 (23.01.2009)