

FRA

Thematic Legal Study on assessment of
data protection measures and relevant
institutions
[Czech Republic]

Pavel Šturma, Věra Honusková
in cooperation with Martin Faix

Prague, Czech Republic
February 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.

Contents

Executive summary	3
1. Overview.....	7
1.1. Data protection legislation.....	7
1.2. Public authorities	9
2. Data Protection Authority	10
2.1. Structure of the Office	11
2.2. Powers of the Office	12
2.3. Guarantees of independence of the Office.....	15
2.4. Awareness raising role of the Office	16
3. Compliance.....	17
4. Sanctions, Compensation and Legal Consequences	21
4.1. Follow-up activities	23
4.2. Personal data protection in employment context	26
5. Rights Awareness.....	28
5.1. Activities of the Data Protection Office	28
5.2. Books on data protection	29
6. Analysis of deficiencies	30
7. Good practices	34
8. Miscellaneous	35
Annexes	36

Executive summary

Overview

- [1]. In the Czech Republic, the protection of personal data is ensured both on the constitutional and statutory levels. The constitutional Charter of Fundamental Rights and Freedoms provides in its Article 10, par. 3, in the context of the protection of human dignity and private and family life, that “everyone has the right to protection against unlawful collecting, publishing or other misuse of personal data”. Moreover, the Czech Republic is a party to several international instruments.
- [2]. The basic legislative framework for the data protection has been set up in the Personal Data Protection Act [Zákon o ochraně osobních údajů; “Act”]. The current law implements in the Czech legal order international and EU principles for protection of personal data. It provides necessary means in order to render effective the right for everyone to protection against unlawful interference with his/her privacy. To this end the Personal Data Protection Act sets up rights and obligations in relation to processing of personal data.

Data Protection Authority

- [3]. The Czech data protection authority, Office for Personal Data Protection [Úřad pro ochranu osobních údajů; “Office”] is an independent, administrative body, which was created on 01.06.2000. The legal basis for its operation is given by the Act. The organizational structure of the Office consists of one President, seven Inspectors and other employees. The resources allocated to the data protection authority (budget, staffing etc.) seem to be sufficient to ensure effective use of the powers given to it. The main areas of powers of the Office can be summarized as supervisory powers and control powers, the powers are stipulated by the Act. The Office may act on its own initiative and also deals with the incentives from the general public. The powers given to the data protection authority correspond more or less to the requirements of Art. 28 of Directive 95/46/EC and seem to be sufficient to ensure effective data protection. There are no concerns about the independence of the Office. The Office is very proactive in public awareness.

Compliance

- [4]. Whoever intends to process personal data as a controller, with the exceptions provided in the Act, shall notify the Office of this intention in writing. The controller may process personal data only with the consent of the data subject. In practice, there is a continuing tendency amongst data controllers to gather personal data on data subjects to an extent greater than necessary in order to fulfill the set purpose. The controller must inform the data subject on his/her right to access his/her personal data, the right to have personal data corrected, as well as other rights. During the control activities performed in 2007, it was ascertained that the mentioned duties were fulfilled either partly or not at all. In 2008 the situation had partly improved.
- [5]. Only the citizens of the Czech Republic may become inspectors of the Office and the conditions that have to be met are essentially the same as for the office of the President of the Office (impeccability, legal capacity, university education, incompatibility of functions in public administration, exclusion of other paid employment and membership in political parties).

Sanctions, Compensation and Legal Consequences

- [6]. The authority competent to order remedy measures and impose sanctions in the Czech Republic is the Office. The competences are set forth in the Act providing general legal framework of data protection in the Czech Republic, as well as in various special laws, containing provisions on data protection.
- [7]. According to provisions of the Act the Office in the case of a violation by a natural person *may* impose sanctions, in the case the breach has been committed by a natural or legal person carrying business, the Office *shall* impose sanctions. The issue of compensation remains widely neglected under the Act and is governed by general laws. Following a complaint or own-motion instigation, the Office may commence an investigation, dismiss the complaint, commence administrative proceedings in the case of a clear breach of applicable provisions, or if not competent, the Office may forward the case to a competent authority. The administrative proceedings lead to a large extent to imposition of sanctions.

- [8]. From a quantitative point of view, the enforcement of data protection legislation depends in general, but not solely on personal initiative of data subjects.

Rights Awareness

- [9]. There are no studies or surveys on awareness regarding data protection law and rights in the population available. The Office runs *inter alia* projects related to personal data protection, there are also books on the issue; those can be counted as possible indicators of awareness regarding data protection law and rights in the population.

Analysis of deficiencies

- [10]. Several problematic issues for the effective data protection in the Czech Republic can be identified. Among the most discussed belong the issue of camera surveillance systems and other systems able to monitor movement of persons (electronic toll systems used on motorways) or use of electronic cards for public services. Data protection aspects are currently an issue also within activities of state authorities and institutions (e.g. project eGovernment). Several violations of laws have been found by the Czech Public Defender for Rights and also by the Office in the activities of Department of Criminology in the context of activities connected with taking DNA samples and the National DNA Database.
- [11]. Certain of the identified deficiencies could be solved by amending the present legislation, such as in the case of camera surveillance systems. However, also continuation of awareness rising appears necessary to improve the effectiveness of personal data protection. As in regard to concrete position of the Office for Personal Data Protection, especially strengthening its role in the legislative process appears necessary.

Good Practice

- [12]. The Office is an approachable modern state authority available by all means to the general public. Its website, its activities towards the public and its friendly attitude may be seen as a good practice. The Office publishes several publications, runs a project aimed at children and youth and also an educational program since 2007 and realizes

many other activities. The financial independence of the Inspectors granted by the Act is also worth mentioning.

Miscellaneous

- [13]. The Office takes part in the activities of the Government Council for Human Rights [Rada vlády pro lidská práva] and of the Government Council for the Information Society [Rada vlády pro informační společnost]. There is a Standing Commission on Privacy Protection [Stálá komise Senátu pro ochranu soukromí] in Senate of the Czech Republic.

1. Overview

- [14]. In the Czech Republic, the protection of personal data is ensured both on the constitutional and statutory levels. The constitutional Charter of Fundamental Rights and Freedoms provides in its Article 10, par. 3, in the context of the protection of human dignity and private and family life, that “everyone has the right to protection against unlawful collecting, publishing or other misuse of personal data”.¹
- [15]. Moreover, the Czech Republic is a party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)² and to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Dataflow (2001).³ It is also a State Party to the Convention on Human Rights and Biomedicine (1997),⁴ therefore it is bound by its Article 10 on ‘Private life and right to information’. As of 25 December 2003, the Czech Republic has been also bound by its declaration under Article 3, par. 2(c) of the 1981 Convention, extending this Convention to the files (sets) of personal data that do not undergo automatic processing.⁵
- [16]. The basic legislative framework for the data protection has been set up in the Act No. 101/2000, on Protection of Personal Data.⁶ There are also other, special legislative acts dealing with particular aspects of data protection.

1.1. Data protection legislation

- [17]. The Act No. 101/2000 on Protection of Personal Data replaced the former Act No. 256/1992, on Protection of Personal Data in Information Systems. The current law implements into the Czech legal order international and EU principles of protection of personal data. It provides necessary means in order to make effective the right of everyone to protection against unlawful interference in privacy. To

¹ Charta základních práv a svobod, vyhlášená pod č. 2/1993 Sb. [Charter of Fundamental Rights and Freedoms, published as No. 2/1993 Coll.].

² Sdělení MZV č. 115/2001 Sb.m.s. [Notice of MFA No. 115/2001 Coll. of Int'l Treaties].

³ Sdělení MZV č. 29/2005 Sb.m.s. [Notice of MFA No. 29/2005 Coll. of Int'l Treaties].

⁴ Sdělení MZV č. 96/2001 Sb.m.s. [Notice of MFA No. 96/2001 Coll. of Int'l Treaties].

⁵ Sdělení MZV č. 28/2005 Sb.m.s. [Notice of MFA No. 28/2005 Coll. of Int'l Treaties].

⁶ Zákon č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších předpisů [Act No. 101/2000 Coll., on Protection of Personal Data, as amended by later laws].

this end the Personal Data Protection Act sets up rights and obligations in relation to processing of personal data.

- [18]. First of all, the Act defines basic terms, such as “personal data” and “sensitive data”, “administrator” and “subject” of personal data. Next, it provides rights and obligations of the administrator in processing of personal data. The Act ensures to subjects of personal data the right of access to information relating to their personal data and remedies in case of violation of their rights. It also sets up conditions under which personal data may be transferred to other States.
- [19]. The Act does not apply to processing of personal data by natural persons and to accidental collecting of personal data where they are not further processed (Sec. 3, paras. 3 and 4, Act No. 101/2000). Certain provisions of the Act do not apply where the matter is regulated by other laws in the field of the security of the Czech Republic,⁷ the defence of the Czech Republic,⁸ the public order and home security,⁹ the prevention, investigation and prosecution of criminal offences,¹⁰ for ensuring an important economic interest of the Czech Republic or the European Union¹¹ and an important financial interest of the Czech Republic or the European Union.
- [20]. There are also other special laws regulating matters related to personal data protection, e.g. the Electronic Communications Act,¹² the Travel

⁷ Cf. ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů [Constitutional Act No. 110/1998 Coll., on Security of the Czech Republic, as amended by later laws], zákon č. 148/1998 Sb., o ochraně utajovaných skutečností, ve znění pozdějších předpisů [Act No. 148/1998 Coll., on Protection of Secret Information, as amended by later laws].

⁸ Cf. zákon č. 222/1999 Sb., o zajišťování obrany České republiky, ve znění pozdějších předpisů [Act No. 222/1999 Coll., on Ensuring Defense of the Czech Republic].

⁹ Cf. zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) ve znění pozdějších předpisů [Act No. 240/2000 Coll., on Crisis Management and amendments to certain laws, as amended by later laws]; zákon č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů [Act No. 283/1991 Coll., on Police of the Czech Republic, as amended by later laws].

¹⁰ Cf. zákon č. 61/1996 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů, ve znění pozdějších předpisů [Act No. 61/1996 Coll., on Certain Measures against Laundering of Proceeds from Crime and amendments to related acts, as amended by later laws]; zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů [Act No. 141/1961 Coll., on Criminal Procedure, as amended by later laws].

¹¹ Cf. zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, ve znění pozdějších předpisů [Act No. 241/2000 Coll., on Economic Measures for Emergencies and amendments to related acts, as amended by later laws].

¹² *Zákon č. 127/2005 Sb., o elektronických komunikacích* [Act No. 127/2005 Coll., on electronic communications].

Documents Act,¹³ the Register of Population Act,¹⁴ the Asylum Act,¹⁵ and Certain Information Society Services Act.¹⁶

1.2. Public authorities

- [21]. The protection of personal data in the Czech Republic falls under the competence of the Office for Personal Data Protection (Úřad pro ochranu osobních údajů). This Office was established by the Act No. 101/2000, on Protection of Personal Data. It has a large scope of competence pursuant to Act No. 101/2000, as well as under special laws. The Office exercises the control and supervision according to attributed competences. It has also the power to investigate and sanction in the administrative proceedings, special administrative offences in the field of personal data processing.
- [22]. On the parliamentary level, the protection of personal data has been dealt with by the Standing Commission on Privacy Protection of the Senate (the higher chamber of the Czech Parliament).

¹³ *Zákon č. 329/1999 Sb. o cestovních dokladech* [Act No. 329/1999 Coll., on travel documents].

¹⁴ *Zákon č. 133/2000 Sb., o evidenci obyvatel* [Act No. 133/2000 Coll., on register of population and birth numbers].

¹⁵ *Zákon č. 325/1999 Sb., o azylu* [The Act No. 325/1999 Coll., on Asylum].

¹⁶ *Zákon č. 480/2004 Sb., o některých službách informační společnosti* [Act No. 480/2004 Coll., on certain information society services].

2. Data Protection Authority

[23]. The Office for Personal Data Protection [Úřad pro ochranu osobních údajů], the Czech data protection authority, was created on 01.06.2000 as an independent body. The legal basis for its operation is given by the Personal Data Protection Act [Zákon o ochraně osobních údajů].¹⁷ Also other laws give powers to the Office, e.g. Electronic Communications Act [Zákon o elektronických komunikacích],¹⁸ Travel Documents Act [Zákon o cestovních dokladech],¹⁹ Register of Population Act [Zákon o evidenci obyvatel],²⁰ Asylum Act [Zákon o azylu],²¹ Certain Information Society Services Act [Zákon o některých službách informační společnosti],²² the Office hereby possesses e.g. competences to impose sanctions pursuant to other laws of the Czech Republic, see Chapter 4 for more information. Some powers arise also from international treaties which form part of the legal order, and from the directly applicable law of the European Communities. The general basis for the protection of everyone's right to privacy is given by Art. 10 (2), (3) of the Charter of Fundamental Rights and Freedoms of the Czech Republic [Listina základních práv a svobod] (i.e. it is stipulated on the constitutional level).²³ The Office also possesses competences to impose sanctions pursuant to other laws of the Czech Republic.

¹⁷ Czech Republic/ Zákon č. 101/2000 Sb., o ochraně osobních údajů (Act No. 101/2000 Coll., on Protection of Personal Data).

¹⁸ Czech Republic/ Zákon č. 127/2005 Sb., o elektronických komunikacích (Act No. 127/2005 Coll., on electronic communications).

¹⁹ Czech Republic/ Zákon č. 329/1999 Sb. o cestovních dokladech (Act No. 329/1999 Coll., on travel documents).

²⁰ Czech Republic/ Zákon č. 133/2000 Sb., o evidenci obyvatel (Act No. 133/2000 Coll., on register of population and birth numbers).

²¹ Czech Republic/ Zákon č. 325/1999 Sb., o azylu (The Act No. 325/1999 Coll., on Asylum).

²² Czech Republic/ Zákon č. 480/2004 Sb., o některých službách informační společnosti (Act No. 480/2004 Coll., on certain information society services).

²³ See Art. 10 (2), (3) of the Charter of Fundamental Rights and Freedoms: (2) Everyone has the right to be protected from any unauthorized intrusion into her private and family life, (3) Everyone has the right to be protected from the unauthorized gathering, public revelation, or other misuse of his personal data. Charter is available on <http://www.psp.cz/cgi-bin/eng/docs/laws/1993/2.html> (in English, accessed on 21.12.2008).

2.1. Structure of the Office

- [24]. As of 1.1.2009, The Office had 98 employees. The organizational structure of the Office consists of one President, seven inspectors and other employees. The President is appointed and recalled by the President of the Czech Republic on the basis of a proposal of the Senate of the Parliament of the Czech Republic. The President is appointed for the period of 5 years, his/ her knowledge, experience and moral qualities are taken into account as a precondition to hold his/ her office properly; there are several other conditions to prevent the conflict of interests – see below. The Inspectors are appointed for a period of 10 years, the procedure of appointment and also the provisions regarding the conflict of interests are analogous to those of the President.
- [25]. The budget of the Office is 101 296 000 CZK for 2009 (EUR 3 835 516,84).²⁴ It is comparable to the budget of e.g. the Office of Public Defender of Rights - Czech Ombudsman [Veřejný ochránce práv], which has similar number of employees. The budget allocated to the Office forms 0,008 % of the budget of the Czech Republic.
- [26]. The resources allocated to the data protection authority (budget, staffing etc.) seem to be sufficient to ensure effective use of the powers given to the data protection authority. Another case may be when there are campaigns on specific topics (camera surveillance systems etc.), which require activity of more employees and then the Office may not have enough capacities to follow the issue.²⁵ However, this situation does not seem to have dramatic effect on the Office and its work, at least the Office follows all the issues which are brought before it and completes all the functions which are given to it by the law.²⁶
- [27]. The Office is divided into three main units: Section of Supervising Activities [Sekce dozorových řízení], Units subordinated to President [Útvary řízené předsedou] and Economic and Operating Section

²⁴ See the budget of the Czech Republic, available at the website of Ministry of Finance, http://www.mfcr.cz/cps/rde/xbcr/mfcr/475_2008_SR_P3_pdf.pdf (accessed 07.01.2009). The equivalent in Euros is calculated on the basis of the Rate of Exchange published in the Official Journal on 06.01.2009, No. 2009/C 2/07.

²⁵ This conclusion is based on the comparison of the range of activities which the Act grants to the Office and the number of campaigns and the extent of them. This opinion was also supported by an NGO Iuridicum Remedium, o.s. (email from Ms JUDr. Ing. Helena Svatošová (Iuridicum Remedium) received on 09.01.2009), www.iure.org (accessed on 02.01.2009).

²⁶ This conclusion is based on the Annual reports [Výroční zprávy] of the Office and the fact, that there are no concerns about the functions of the Office expressed by the Parliament and Government of the Czech Republic, to which the Annual report is submitted.

[Sekce ekonomická a provozní] which coordinate operation of several subordinated departments, including Inspectors, who carry out the control activities.

- [28]. The Office may act on its own initiative when there is a justified concern that the Act might be breached in processing of personal data (Sec. 17 (1) of the Act). The controllers may investigate, they may enter the property of the controllers and processors, they may ask information and documentation etc. (Sec. 31 of the Act). The Office has a plan of controls and acts upon its own initiative and also acts upon incentives from the general public. It can be followed from the annual reports and statistics that the Office acts upon its own initiative less than upon the incentives from the general public. But it needs to be said that the general public is very active and there are also incentives and complaints on the main issues of concern – where the Office might have been active on its own initiative – given by the public. The Office is very proactive in public awareness and the general public is active and the Office then technically speaking reacts and acts upon complaints and not on its own initiative. More powers to the Office upon the state authorities would be a possibility how to strengthen the Office in the future.
- [29]. The Office is a member of the WP 29 and the opinions represent a source of inspiration for the interpretation of the national legislation implementing the EU legislation on data protection. But they are not legally binding.

2.2. Powers of the Office

- [30]. The main areas of powers of the Office can be summarized as supervisory powers and control powers. The Office deals mainly with the issue of personal data collecting, personal data processing and personal data preserving. The powers of the Office are stipulated by the Act (mainly Sec. 29): The Office mainly (a) supervises fulfilling of the obligations provided by the law in personal data processing; (b) keeps the register of personal data processing; (c) accepts incentives and complaints on the breach of obligations provided by the law in personal data processing and informs about their settlement; (d) prepares annual reports on its activities and makes it accessible to the public; (e) exercise other competences stipulated by the law; (f) deals with administrative offences and impose fines; (g) ensures fulfilment of international treaties and directly applicable law of the European Communities, (h) provides consultations, (i) co-operate with similar authorities in other countries, with the European Union institutions

and with bodies of international organizations; it also fulfils the notification duty towards the European Union institutions.

- [31]. Do the powers given to the data protection authority correspond to the requirements of Article 28 of Directive 95/46/EC? The public authority responsible for monitoring the application of the provisions pursuant to this Directive is the Office. The Office is independent (see below in a separate sub-chapter of this report). The Office has the powers regarding fulfilment of the Art. 28 (3) of the Directive. The Office is given investigative powers and it may investigate upon its own initiative or upon incentive from other subjects. The Office can also intervene; it may order blocking, erasure or destruction of data (the Act gives the Inspector the powers to determine which measures shall be adopted in order to eliminate the shortcomings). The Office also runs a register of controllers; the controllers may not collect data without an approval of the Office. The Office may then control their activities in the area of data processing and other obligations pursuant to the Act. The Office initiates proceedings upon its own initiative when a justified concern of the breach of the Act in the area of personal data processing arises. The Office can open an administrative procedure when the obligations given by the Act are violated, it can also bring the violation to the attention of the police (bring complaint and thus start criminal proceedings). The Office can also act as a party before a court. The Office moreover hears claims and informs the persons of the outcome of the claim (see more details below). The Office also issues (not legally binding) positions, which are made public on its website and also via press releases. It also issues annual reports, which are submitted for information purposes to the Chamber of the Deputies and the Senate of the Parliament of the Czech Republic and to the Government of the Czech Republic within 2 months of the end of the budgetary year, and are also published on the website of the Office. The Office cooperates with authorities of other Member States and the Act also contains the provisions on transfer of personal data. The powers given to the data protection authority are in compliance with the Art. 28 of the Directive.
- [32]. The Office is consulted on draft legislation which may have an impact on the protection of personal data; the draft laws are sent to the Office pursuant to the Sec. 5 of the Governmental Legislation Rules [Legislativní pravidla vlády].²⁷ The Council may give comments and

²⁷ Czech Republic/ Legislativní pravidla vlády schválená usnesením vlády ze dne 19. března 1998 č. 188 (Governmental Legislation Rules confirmed by the Governmental Resolution of 19.03.1998, as changed), available at http://www.vlada.cz/assets/cs/rvk/lrv/Pravidla/legislativn_pravidla_vl_dy.pdf (accessed on 02.01.2009).

suggestions to the Government regarding e.g. changes in the law. But the Office itself cannot propose drafts and draft amendments to laws, so it may be said that its role is not strong enough to propose the legislation, only to comment upon it (which nevertheless is in compliance with the Art. 28 of the Directive). The Office is also a member of the Government Council for Human Rights [Rada vlády pro lidská práva] where it can raise issues of concern and give incentives for the Council's debates.

- [33]. The remit of the data protection authority is limited by the remit given by the Directive 95/46/EC. The limits may be seen in the powers over the personal data processing in the state authorities (as they are stipulated by the Directive in its Art. 3 (2)). Thus some provisions of the Act do not apply to processing of personal data which is necessary to fulfil obligations of the controller provided by special laws to ensure e.g. security and defence of the Czech Republic, public order and internal security, prevention, investigation, detection and prosecution of criminal offences, important or financial and economic interest of the Czech Republic or of the European Union etc. Accordingly some provisions of the Act also do not apply to the processing of personal data by a natural person in the course of a purely personal or household activity.
- [34]. The Act is a general norm; it does not contain detailed areas of activities. It seems to be a proper frame, when we see the technical developments of the last years. If the areas of activities were more specific, the law would have been changed and reformed often.
- [35]. The Office may act on its own initiative when there is a justified concern that the Act might be breached in processing of personal data (Sec. 17 (1) of the Act). The controllers may investigate, they may enter the property of the controllers and processors, they may ask information and documentation etc. (Sec. 31 of the Act). The Office has a plan of controls and acts upon its own initiative and also acts upon incentives from the general public. It can be followed from the annual reports and statistics that the Office acts upon its own initiative less than upon the incentives from the general public. But it needs to be said that the general public is very active and there are also incentives and complaints on the main issues of concern – where the Office might have been active on its own initiative – given by the public. The Office is very proactive in public awareness and the general public is active and the Office then technically speaking reacts and acts upon complaints and not on its own initiative. More powers to the Office upon the state authorities would be a possibility how to strengthen the Office in the future.

2.3. Guarantees of independence of the Office

- [36]. The guarantees of independence are granted by the Personal Data Protection Act [Zákon o ochraně osobních údajů] itself, which stipulates (a) that the Office is an independent body, that the Office acts independently in its activities and is only abide by the Personal Data Protection Act and other legal regulations, (b) the activities of the Office may be interfered with only on the basis of law, (c) also the financial independence is stipulated, because the activities of the Office are paid from a special part (chapter) of the state budget (Sec. 28 of the Act). The independence is also ensured (d) by the way how the President [Předseda] is chosen (see Chapter 3); and by the (e) provisions on the prevention of the conflict of interests given to him by the Act (see Chapter 3). The independence is ensured also by the process of selection of the Inspectors (same procedure as for the President applies) and analogous provisions about the conflict of interest apply also to them (Sec. 33 (1), Sec. 34 of the Act). The independence is also ensured by the salary range of the President and the Inspectors, which is comparable to the President of the Supreme Audit Office and the members of the Supreme Audit Office. The Inspectors and authorized employees may also not carry out inspections in case when there are reasonable doubts about their prejudice, with respect to the matter of control or a relationship between the controlled and controlling persons [Kontrolující].²⁸ The person holding the office of the President of the Office and inspectors (f) must also meet the conditions prescribed by a special legal regulation, the so-called Lustration Act²⁹, which prohibits the members of power elites and armed bodies of the former non-democratic regime to hold selected offices in the state administration, territorial self-administration and armed forces. There are no concerns about the independence of the Office.

²⁸ The term controlling person is the term which is being used by the official translation of the Act by the Office. The Czech term literally means “the person who controls”, however e.g. a term officer can be used also.

²⁹ Czech Republic/ Zákon č. 451/1991 Sb., kterým se stanoví některé další předpoklady pro výkon některých funkcí ve státních orgánech a organizacích České a Slovenské Federativní Republiky, České republiky a Slovenské republiky (Act No. 451/1991 Coll., laying down some preconditions for the exercise of certain functions in state bodies and organizations of Czech and Slovak Federal Republic, Czech Republic and the Slovak Republic (the so -called Lustration Act), as amended.

2.4. Awareness raising role of the Office

- [37]. The obligations deriving from the Act are listed in the Act. The Act as such is publicly available and also the particular obligations are available via website of the Office. The Office also issues leaflets with information. The positions of the Office are available to the public via web site.³⁰ The web site contains also the main decisions of the courts in Czech Republic and also of the courts abroad (European Court of Human Rights, European Court of Justice etc.) in the respective area. Also a register of the subjects which process the data is available via this web site.
- [38]. The Office is very active in awareness raising role. It runs a very detailed website,³¹ where not only the positions of the Office are published, but also the main decision of the Czech courts can be found there. The Office also organizes competitions through which the young generation learns about their rights (My Privacy! Don't Look, Don't Poke About It!) and also educational program (Protection of personal data in education). The Office also publishes Informational Bulletin.³²

³⁰ The English version of the web site is available on <http://www.uoou.cz/index.php?l=en&m=bottom&mid=01&u1=&u2=&t=>

³¹ See <http://www.uoou.cz/index.php?l=en&m=bottom&mid=01&u1=&u2=&t=> (English, accessed 02.01.2009).

³² The Bulletins can be found at <http://www.uoou.cz/index.php?l=cz&m=left&mid=10:03&u1=&u2=&t=> (accessed on 02.01.2009).

3. Compliance

- [39]. Pursuant to the Personal Data Protection Act [Zákon o ochraně osobních údajů], whoever intends to process personal data as a controller, with the exception provided in the Act³³, shall notify the Office of the intention in writing.³⁴ Under the Act the “controller” [Správce] shall mean any entity that determines the purpose and the means of personal data processing, carries out such processing and is responsible for such processing. The controller may empower or charge a “processor” [Zpracovatel] to process personal data unless a special Act provides otherwise. The notification obligation applies exclusively to controllers (not to processors or other persons, who are concerned with personal data processing). Since the end of 2006 the controllers may lodge the registration notification electronically using a registration form available on the Office web site.³⁵ The registration form can be sent in electronically or by mail. There is no obligation to use the special form mentioned above, the notification letter must only fulfil all the statutory requirements (Sec. 16 (2) of the Act). A controller may start the personal data processing on the day on which it was registered by the Office or after expiration of 30 days from the delivery of the notification to the Office. Upon a controller's request, the Office shall issue a certificate of registration. According to the Sec. 16 of the Act the registration process is not a license system,³⁶ therefore the certificate cannot be claimed to be a proof that the Office has revised the proceeding. The fact that the proceeding is in accordance with the law may only be proven by supervisory control

³³ See Sec. 18 of this Act.

³⁴ See Sec. 16 of the Act.

³⁵ See <http://www.uoou.cz> (English version at <http://www.uoou.cz/index.php?l=en&m=bottom&mid=01&u1=&u2=&t=>; accessed on 02.01.2009).

³⁶ Cp. approval procedure under the Sec. 27 (4) of this Act, if the controller intends to transfer any personal data to other countries, it is in certain cases required to seek a relevant permit from the Office in keeping with Article 27 of the Act. In the first place, it is not allowed to restrict any free movement of personal data if such personal data are to be transferred to a member state of the European Union. To other (the so-called third) countries personal data may be transferred if the prohibition to restrict free movement of personal data is ensuing from an international treaty the ratification of which was approved by the Parliament and which is binding the Czech Republic or such personal data are transferred on the basis of a decision of an institution of the European Union. In cases other than the two above-described ways of transfer of personal data, controllers shall seek with the Office permission to the transfer thereof. The Office shall launch an administrative proceeding aimed at reviewing all circumstances relating to the personal data transfer, in particular the source, final destination, and categories of the transferred personal data, the purpose and period of their retention, and shall issue a decision. The application shall be processed by the Office pursuant to of Act No. 500/2004 Coll., the Administrative Code, within 30 days, or within 60 days if the case is more difficult.

(see below). It should also be noted that quite a wide range of processing are exempted from the notification obligation (Sec. 18 (1) of the Act; the notification obligation pursuant to Article 16 shall not apply to processing of personal data e.g. that are part of data files publicly accessible on the basis of a special Act etc.).

[40]. Only the citizens of Czech Republic may become inspectors of the Office³⁷ and the conditions that have to be met are essentially the same as for the office of the President of the Office (impeccability, legal capacity, incompatibility of functions in public administration, exclusion of other paid employment and membership in political parties). Inspectors shall also be appointed and recalled by the President of Czech Republic on the basis of a proposal of the Senate. They are appointed for a period of 10 years, even recurrently and they may be recalled if they no longer meet one or more of the conditions for the appointment. The person holding office of the President of the Office and inspectors must also meet the conditions prescribed by a special legal regulation, the so-called Lustration Act [Lustrační zákon, see also above in Chapter 2], which prohibits the members of power elites and armed bodies of the former non-democratic regime to hold selected offices in the state administration, territorial self-administration and armed forces. It may be said that the method of appointing the President of the Office and the inspectors complies with the required independence. Other employees of the Office do not have to comply with any additional requirement but the provisions of the Labour Code and the internal organizational rules. Inspectors and authorized employees may not carry out inspections in case when there are reasonable doubts about their prejudice, with respect to the matter of control or a relationship between the controlled and controlling persons.

[41]. The controller may process personal data only with the consent of data subject³⁸. The Act does not provide for an obligatory form for the consent, as of in written, for example. The Act regulates exemptions, under which the controller may process personal data without the consent of data subject (e.g. if he provides personal data on a publicly active person; see Sec. 5 of the Act). In the case of an obligatory consent for the processing of personal data the regulation is stricter. Sensitive data³⁹ may be processed only if the data subject has given an

³⁷ See Article 33, 34 of this Act.

³⁸ Consent of data subject shall mean a free and informed manifestation of will of the data subject the content of which is his assent to personal data processing; see Article 4 (n) of this Act.

³⁹ The sensitive data mean personal data revealing nationality, racial or ethnic origin, political attitudes, trade-union membership, religious and philosophical beliefs, conviction of a criminal act, health status and sexual life of the data subject and genetic data of the data

express consent for the processing. Sensitive data may be processed without consent only in cases listed in the Act (e.g. it is necessary in order to preserve the life or health of the data subject). When giving the consent the data subject must be (in both cases) informed about the purpose of the processing and what particular data is the object of the consent, who is the controller and for what time period. The controller must be able to prove the data subject's consent for personal data processing during the whole period of processing. While collecting personal data subject must be informed on his rights and on who can access his personal data. In case of collecting sensitive personal data the controller must do so in advance. Upon data subject's request the controller must grant information on the processing of personal data, on its purpose, on personal data that are the object of the processing including the source, the character of the eventual automated processing and about categories of recipients. The data subject may request explanation of the processing of personal data in case the subject believes the processing is not carried out properly and has the right to claim remedy. It is always necessary to ensure that the rights of the data subject are not infringed upon, in particular the right to preservation of human dignity, and to ensure that the private and personal life of the data subject is protected against unauthorized interference. Legal regulation of duties of registration of data processing operations in the Czech Republic is in compliance with the law of the European Communities and international agreements binding Czech Republic⁴⁰.

- [42]. So far 33482⁴¹ notifications were filed at the Office with 26354 registered processing⁴². In practice the Office encounters cases when the registration of data processing is requested, but the data meet the conditions for exemption from the notification obligation⁴³. According to the Office, there is still a problem with a fact, the obliged entities the registration is mostly perceived as factual consent to the implementation of the notified activity. In 2008 the situation has

subject; sensitive data shall also mean a biometric data permitting direct identification or authentication of the data subject; see Sec. 4 (b) of this Act.

- ⁴⁰ Cf. especially 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 and Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, CETS No. 108).
- ⁴¹ Data valid on 08.09.2008. The Office for Personal Data Protection, Information Bulletin No. 3/2008, page 3 (Czech version only), available at http://www.uoou.cz/zpravodaj/bulletin_2008_03.pdf (accessed on 07.01.2009).
- ⁴² The Office for Personal Data Protection, The Public Register of Personal Data Processing (Czech version only), available at <http://www.uoou.cz/int/registr-cz.php> (accessed on 02.01.2009).
- ⁴³ Mainly concerns cases when the personal data processing is necessary in order to carry out the legal duties provided for in special Acts that can be subordinated under the Exclusion of notification duty provision under Article 18 (1b) of the Act.

improved in comparison with the 2007⁴⁴. In practice, there is a continuing tendency amongst data controllers to gather personal data on data subjects to an extent greater than necessary in order to fulfil the set purpose.⁴⁵ The mentioned fact was noticed not only in the private sector, but also in the public sector. Other very frequent violations of the duties of data controllers and eventually data processors include failure to fulfil the information duty pursuant to Article 11 of the Personal Data Protection Act, that imposes certain duties on the controller, such as the duty to inform the data subject during the data processing about the scope and purpose of personal data processing, by whom and in what manner the personal data will be processed and to whom the personal data may be disclosed, within collection of personal data, unless the data subject is already aware of this information. The controller must inform the data subject on his right to access his/her personal data, the right to have personal data corrected, as well as other rights. During the control activities performed in 2007, it was ascertained that the mentioned duties were fulfilled either partly or not at all. In 2008 the situation had partly improved.⁴⁶

⁴⁴ *Výroční zpráva Úřadu pro ochranu osobních údajů* (Annual Report the Office for Personal Data Protection for 2007), page 9, available at http://www.uoou.cz/rep_2007.pdf, (accessed on 02.01.2009). The opinion was approved by representatives of the Office for Personal Data Protection during a meeting on 08.01.2009.

⁴⁵ See the Annual Report, p. 9.

⁴⁶ The Office for Personal Data Protection, Annual Report 2007, page 9, available at http://www.uoou.cz/rep_2007.pdf, (accessed on January 4, 2009). The opinion was approved by representatives of the Office for Personal Data Protection during a meeting on 08.01.2009.

4. Sanctions, Compensation and Legal Consequences

- [43]. Provisions on remedy measures, sanctions and legal consequences can be found in the Personal Data Protection Act [Zákon o ochraně osobních údajů] providing the general legal framework for personal data protection in the Czech Republic, but increasingly also in other special laws, which contain provisions on administrative offences connected to personal data protection and thus establish new competences of the Office for Personal Data Protection [Úřad pro ochranu osobních údajů]. This is caused due the position of the Office as a central administrative authority for data protection issues.
- [44]. In the Personal Data Protection Act, measures for remedy are set forth in Sec. 40 par. 1 of the Personal Data Protection Act providing that if a controlling person finds a breach of obligations imposed by the Act, the inspector shall determine which measures shall be adopted in order to eliminate the established shortcomings and set a deadline for their elimination. The controlled person is then pursuant to Sec. 40 par. 3 of the Personal Data Protection Act obliged to submit a report on the adopted measures within the set deadline. If the measures are not adopted within the set deadline, a fine may be imposed on the controlled person. It has to be noted that pursuant to Sec. 41, the Správní řád [Administrative Code]⁴⁷ governs proceedings in matters regulated by the Personal Data Protection Act, unless the Personal Data Protection Act provides otherwise, such as in Sec. 40 para. 2. This provision concerns the case, when destruction of personal data as a remedy measure has been ordered.
- [45]. Chapter VII of the Personal Data Protection Act concerns penalties: Sec. 44 stipulates elements of offences under the Act and subsequent fines, which can be imposed on natural persons. Sec. 45 concerns natural and legal persons, who carry business. This provision lays down elements of administrative offences under the Personal Data Protection Act, as well as the fines, which shall be imposed on the perpetrator. A difference in the wording of Sec. 44 and Sec. 45 may be noted at this point: Pursuant to Sec. 44 a fine *may* be imposed on a natural person, whereas pursuant to Sec. 45 a fine *shall* be imposed on

⁴⁷ Czech Republic/ Zákon č. 500/2004 Sb., o správním řízení (správní řád) [Act No. 71/1967 Coll., Administrative Code], available at: <http://portal.gov.cz/wps/portal/s.155/701?kam=zakon&c=500/2004> (Czech only; accessed on January 9, 2009).

a natural or legal person carrying business. An exculpation and limitation is possible under the Act, however, only for natural and legal persons carrying business.⁴⁸ It also has to be mentioned that the only provision concerning compensation payments for property damage is Sec. 21 par. 5.⁴⁹ The wording of these provisions is rather confusing – for claims concerning other than property damages it refers to the Civil Code⁵⁰ but the topic of property damage claims remains further neglected in the provision itself, as well as in the whole Personal Data Protection Act. Sec. 26 further stipulates that general regulation of liability for damage shall apply to matters not specified by the Act, referring to the Civil Code⁵¹ and the Commercial Code⁵².

- [46]. The Personal Data Protection Act contains further provisions on legal consequences. For example, pursuant to Sec. 17a the Office shall decide on revocation of the registration, if according to the Office the controller, whose notification of data processing has been registered, breaches the conditions stipulated by the Act. Furthermore Sec. 21 of the Personal Data Protection Act sets forth situations, in which a data subject has the right to apply directly to the Office.
- [47]. The Office also possesses competences to impose sanctions pursuant to other laws of the Czech Republic. For example, the Certain Information Society Services Act [Zákon o některých službách informační společnosti],⁵³ stipulates in Section 10(1) that supervision over the compliance with the Act in the area of dissemination of commercial communications shall be executed by the Office for

⁴⁸ Sec. 46 para. 1 (exculpation) and Sec. 46 para. 3 (limitation) of the Personal Data Protection Act.

⁴⁹ Sec. 21 para. 5 of the Personal Data Protection Act stipulates that if the data subject incurred other than property damage as a result of personal data processing, the procedure pursuant to a special Act shall be followed when lodging a claim.

⁵⁰ Czech Republic/ Zákon č. 40/1964 Sb., občanský zákoník [Act No. 40/1964 Coll., Civil Code], available at:

http://portal.gov.cz/wps/portal/_s.155/701?number1=40%2F1964&number2=&name=&text=
(in Czech only) (last accessed on 10. January 2009).

⁵¹ Czech Republic/ Zákon č. 40/1964 Sb., občanský zákoník [Act No. 40/1964 Coll., Civil Code], available at:

http://portal.gov.cz/wps/portal/_s.155/701?number1=40%2F1964&number2=&name=&text=
(in Czech only) (last accessed on 10. January 2009).

⁵² Czech Republic/ Zákon č. 513/1991 Sb., obchodní zákoník [Act. No. 513/1991 Coll., Commercial Code], available at:

http://portal.gov.cz/wps/portal/_s.155/701?number1=513%2F1991&number2=&name=&text=
(in Czech only) (last accessed on 10. January 2009).

⁵³ Czech Republic/ Zákon č. 480/2004 Sb., o některých službách informační společnosti [Act No. 480/2004 Coll., on certain information society services and the amendment to certain other acts (Certain Information Society Services Act)], available at:

http://portal.gov.cz/wps/portal/_s.155/701?number1=480%2F2004&number2=&name=&text=
(in Czech only) (last accessed on 09. January 2009).

Personal Data Protection. Pursuant to Sec. 12(5), the supervisory body shall impose and collect fines for administrative offences pursuant to this Act. The Office is also competent to discuss administrative offences and impose fines in the area of special processing of personal data, as stipulated in various laws.⁵⁴

- [48]. According to the Personal Data Protection Act, the proof of intent or negligence is of importance only in the context of deciding on the amount of a fine imposed as a consequence of committing an administrative offence pursuant to the Act. Pursuant to Sec. 46(2), the Office for Personal Data Protection when deciding on the amount of a fine shall take into account *inter alia* the seriousness, manner and the circumstances under which the infringing behaviour was committed. The Office applies this provision in practice, as can be shown on cases, in which the Office did not impose sanctions despite, even marginal, breaches of personal data protection laws.⁵⁵

4.1. Follow-up activities

- [49]. In accordance with the Personal Data Protection Act, as well as other applicable administrative laws, the Office for Personal Data Protection may take four types of action following a complaint or identified problem. In the case the Office suspects a breach of applicable legislation, which it is competent to monitor the compliance with, the Office may commence a control, i.e. initiate an investigation pursuant provisions of Chapters IV and V of the Personal Data Protection Act. Secondly, if the facts of the case fulfil the conditions of Sec. 44 and Sec. 45 of the Personal Data Protection Act, the Office will commence administrative proceedings. Thirdly, the Office may dismiss the complaint with notification or fourthly, in the case the Office regards itself as not competent in the particular case, it will forward it to the competent authority.

⁵⁴ Czech Republic/ *Zákon č. 133/2000 Sb., o evidenci obyvatel* [Act No. 133/2000 Coll., on register of population, available at http://portal.gov.cz/wps/portal/_s.155/701?number1=133%2F2000&number2=&name=&text= (in Czech only) (last accessed on 09. January 2009) stipulates in Article 17e(6) that any administrative offences pursuant to that Act shall be reviewed in the first instance by the Office for Personal Data Protection; *Zákon č. 329/1999 Sb., o cestovních dokladech* [Act No. 329/1999 Coll., on travel documents], available at: http://portal.gov.cz/wps/portal/_s.155/701?number1=329%2F1999&number2=&name=&text= (in Czech only) (last accessed on 09. January 2009) stipulates in Section 34a(4) and in Section 34c(4) that the Office for Personal Data Protection shall be the authority competent in the first instance for proceedings concerning minor offences and administrative offences relating to unauthorised processing of information stored on biometric data carriers.

⁵⁵ Cp. *Výroční zpráva 2007* [Annual report 2007], p. 18-20, available at: http://www.uoou.cz/rep_2007.pdf (available in English) (last accessed 09.01.2009).

- [50]. The Office is also competent for proceedings pursuant to Sec. 17 of the Personal Data Protection Act, which are pursued ex officio in cases where a justified concern arises on the basis of a lodged notification of personal data processing that this processing could be at variance with the Act.⁵⁶ The legal consequence of such proceedings, in the case provisions of the Act have been violated, is not a sanction, but disapproval with processing of personal data.
- [51]. There is no information available to the authors of this study concerning the compensations claimed or reached in personal data protection cases. This is due the fact that the Office is not competent to decide about compensations and according to provisions of the Personal Data Protection Act, compensations have to be claimed by data subjects pursuant to general law provisions regulating liability for damage and indemnification.⁵⁷ As in regard to case law, there is no in print or electronic publication of decisions of lower courts in the Czech Republic; only decisions of higher Courts (such as of the Constitutional Court, the Supreme Administrative Court, etc.) are available. Among decisions available to the authors, no data protection cases concerning claimed or reached compensations could be found. As only data subjects can claim compensations and the Office does not play any role in this regard, it can be argued, that enforcement of personal data protection legislation through compensations payments depends always from personal initiative of data subjects.
- [52]. The situation concerning sanctions may be assessed on the basis of available data. The Office possesses the competence to impose sanctions pursuant to several laws.⁵⁸ In 2007, the Office handled totally 305 instigations including instigations based on Offices' own motion controls or received as data subject complaints. In 82 cases administrative penalty proceedings were commenced, leading in 43 cases to penalty imposition; 21 cases were referred to the competent body before commencement of proceedings, and in 18 cases proceedings did not continue, as according to the Office a tort has not been committed.⁵⁹ From the 43 cases, in which a fine was imposed, in 32 cases the fine has been imposed with legal force. Thus on the basis of the aforesaid it can be argued that the follow up activities of the

⁵⁶ Practically all such administrative proceedings pursued in 2007 were concerned with notified deployment of camera surveillance systems (37 in schools, 22 in enterprises, 8 in apartment buildings, 6 in hospitals and 6 in public administrative bodies).

⁵⁷ Sec. 25 of the Personal Data Protection Act.

⁵⁸ The Office is competent for penalty proceedings pursuant to provisions of the Personal Data Protection Act, Register of Population Act, Act on Conflict of Interests and Certain Services of Information Society Act.

⁵⁹ *Výroční zpráva 2007* [Annual report 2007], available at: http://www.uoou.cz/rep_2007.pdf (available in English) (last accessed 09.01.2009).

Office as responsible authority lead to sanctions to a great extent, however, not solely.

[53]. As it can be inferred from the annual reports and statistics, a high number of investigations carried out by the Office are based on personal initiative of data subjects, and only few are own-motion investigations of the Office for Personal Data Protection. However, this quantitative disproportion has to be considered also from qualitative point of view. Investigations based on personal initiative of subjects are often less time-consuming and not as extensive as the own-motion investigations of the Office. The last mentioned investigations are in most cases in-depth investigations being carried out in large institutions, such as banks etc. Thus, regarded from *quantitative* point of view only, it could be argued that enforcement of data protection legislation in the Czech Republic depends to greater extent on personal initiatives of data subjects.

[54]. A considerable increase of individual complaints received by the Office every year shows a continuously growing awareness among the wide public about personal data protection and related legal rights.⁶⁰ This might be considered also as a result of activities of the Office, which include *inter alia* providing data subjects, as well as e.g. attorneys with legal advice and consultation. Sec. 29 of the Personal Data Protection Act stipulates the competences of the Office, stating under Sec. 29/h that the Office shall provide consultations in the area of personal data protection. This provision is being used extensively⁶¹ not only by data subjects, but last but not least by attorneys, often seeking an in-depth analysis of a personal data protection related problem.⁶² The Office provides legal advice and consultation even beyond its obligations set forth in the Act: The Czech administrative law provisions do not require an authority to state reasons for the decision if dismissing a case. However, the Office even in such cases, in which the investigation was based on an individual complaint but the complaint was dismissed, states the reasons for its decision and provides legal advice and consultation to the data subject concerned. Taking into account also publications issued by the Office in print and electronically to inform the wide public about various personal data

⁶⁰ This has been also confirmed by JUDr. Zdenek Koudelka, director of the Department for Contacts with the Public of the Office for Personal Data Protection, in a personal interview on 08. January 2009.

⁶¹ The Office provides consultations by all available means including telephone, email and in writing. In 2007 for example, the Office answered daily on average 35 telephone inquiries, provided in 60 cases extensive personal consultation (50 per cent more than in 2006) and a total of 1 674 inquiries were handled by email.

⁶² Personal interview with JUDr. Zdenek Koudelka, the Office for Personal Data Protection (08. January 2009).

protection issues, it might be argued that data subjects are sufficiently informed and assisted by the Czech data protection authority.

- [55]. In regard to NGOs providing assistance and information to data subjects in the Czech Republic, there is only one such NGO dealing with personal data protection systematically – Iuridicum Remedium. Even if this organization provides also legal representation in data protection cases, it does so only in exceptional cases of strategic importance and concerning workers rights.⁶³ Providing information and legal consultation belongs on the other hand to regular activities of Iuridicum Remedium.
- [56]. Legal aid and legal representation in data protection cases before administrative authorities and before courts are not institutionalised by a special law in the Czech Republic. The financial risk of legal procedures (attorney fees, etc.) in data protection cases before the administrative authorities bears the data subject itself. As the Office is an administrative authority, the procedures commenced before it are not subject to any fees. If one of the parties affected in the case, after exhausting prescribed administrative procedures, wishes to take the case to the court, general legal provisions concerning court fees, attorney fees etc. apply.⁶⁴ According to these provisions, the Court decides on the costs of the trial, whereas usually the party losing the case bears such costs.

4.2. Personal data protection in employment context

- [57]. When considering protection of personal data in the context of employment, it has to be noted that the Personal Data Protection Act provides general legal framework for personal data protection in the Czech Republic. However, there are several special laws and law provisions applicable, such as those of the Labour Code⁶⁵. Because of this legislative heterogeneity it is not possible for the authors of the report to consider all legal provisions ensuring protection of personal

⁶³ Email from Ms. JUDr. Ing. Helena Svatošová (Iuridicum Remedium) received on 09. January 2009.

⁶⁴ Czech Republic/ *Zákon č. 549/1991 Sb., o soudních poplatcích* (Act No. 549/1991 Coll., on Court Fees), *Vyhláška Ministerstva spravedlnosti č. 177/1996 Sb., o odměnách advokátů a náhradách advokátů za poskytování právních služeb (advokátní tarif)* (Regulation of the Ministry of Justice No. 177/1996 Coll., on Lawyers Tariff).

⁶⁵ See e.g. Sec. 312, Sec. 137 of the Labour Code. *Zákon č. 262/2006 Sb., zákoník práce* (Act No. 262/2006 Coll., Labour Code), available at: http://portal.gov.cz/wps/portal/_s.155/701?number1=262%2F2006&number2=&name=&text= (in Czech only) (last accessed on 10. January 2009).

data in the context of employment. Furthermore, there is nearly no discussion on this topic. Thus, the protection is ensured by the general law governing personal data protection – the Personal Data Protection Act. In the Annual Report 2007, the Office dealt to a small extent with the issue in reaction to controls carried out in 2007.⁶⁶ In the Annual Report 2007, the Office provided *inter alia* the listing of personal data, which are necessary to collect and to process for the employer in order to fulfil his obligations in relation to the employees. It might be noted, that the unions and works councils provide consultations to their members and other workers in questions regarding data protection, however, the unions and works councils do not have any role in monitoring compliance with the applicable legislation – the only body responsible for monitoring under the Personal Data Protection Act is the Office for Personal Data Protection.

⁶⁶ Výroční zpráva 2007 [Annual report 2007], p. 18-20, available at: http://www.uouu.cz/rep_2007.pdf (available in English) (last accessed 09.01.2009).

5. Rights Awareness

- [58]. There are no studies or surveys on awareness regarding data protection law and rights in the population available. The books and other possible indicators of awareness regarding data protection law and rights in the population are listed below.

5.1. Activities of the Data Protection Office

- [59]. The Office runs projects related to personal data protection. There were e.g. two of them in 2008. A first one was aimed at the children and youth, it was a 2nd year of a competition called “My Privacy! Don’t Watch, Don’t Poke!”. There were 233 competitors in 2008 competing with their paintings and essays in three age categories: 7-11, 12-15 and 16-18. The Office also runs an educational program called “Protection of Personal Data in Education” since 2007. This program is approved by the Ministry of Education and is intended for teachers. The seminars also touch the main issues regarding the specific subjects that the teachers deal with. The history of privacy and the influence of totalitarian regimes on privacy are destined for historians, safety on internet or electronic signature for mathematics, DNA taking and fingerprints databases for doctors etc.⁶⁷
- [60]. When the Office deals with an important issue (Camera surveillance system in apartment houses, camera surveillance system at schools etc.), its procedure is almost in a form of a campaign (in a positive meaning of the word). The Office uses of course all the legal means with which it dispose to reach the situation which would be in compliance with the law (e.g. to use the cameras in accordance with the law) and besides that it makes all its opinions and steps public (when it is not restricted by the law) by the website, Bulletins, leaflets and by other media –TV, radio etc. Its method may be described as successful, because people seem to care about their rights more. There is an example of the issue of using the camera surveillance system at schools, where the students themselves made the incentives.

⁶⁷ For this project and for the project “My privacy! Don’t watch, don’t poke!” was the Office awarded the “Prize to Data Protection Best Practices in European Public Service” by the Personal Data Protection Agency in Madrid; for more information see: <http://www.uouu.cz/index.php?l=en&m=bottom&mid=01:12&u1=&u2=&t=> (in English, accessed on 21.12.2008).

5.2. Books on data protection

- [61]. There are several books, which are focused on the relevant issue, including commentaries to the Personal Data Protection Act. The newest and main books are listed below.
- [62]. The newest one is a handbook Maštalka, J.: *Osobní údaje, právo a my* [Personal data, law and us] Praha, C.H.Beck 2008, which describes and explains content of the main principles of the data protection law. It uses a case-law to clarify the theory.
- [63]. A book by Matoušová M., Hejlik L.: *Osobní údaje a jejich ochrana*, [Personal Data and Its Protection] ASPI- Wolters Kluwer, Praha, 2008 gives detailed interpretation of the Data Protection Act. It is addressed also to the general public, not only experts.
- [64]. There is a commentary of the Act, which responds to the needs of practitioners: Kučerová, A., Bartík, V., Peca, J., Neuwirt, K., Nejedlý, J.: *Zákon o ochraně osobních údajů (komentář)* [The Personal Data Protection Act (A Commentary)], C. H. Beck, Praha 2003, 388 s. The commentary contains a text of the act, interpretation of the main principles of the act, commentary to its provisions and also parts of other relevant Czech laws, and laws of the European Communities.
- [65]. The book by Mates, P.: *Ochrana osobních údajů* [Personal Data Protection], Karolinum, Praha, 2002 analyses the right to information on one side and the right to data protection on the other side. The author also comments on some provisions of the Personal Data Protection Act.

6. Analysis of deficiencies

[66]. There is a general upward trend of situations in the Czech Republic, in which data subjects are *de facto* not free to decide, whether or not to consent to collection and processing of their personal data. This problem arises in the context of steady increase of camera surveillance systems monitoring public places, as well as for example in the context of electronic cards for public services, increasingly used more and more in the Czech Republic. The last mentioned have been in focus of the Office for Personal Data Protection [Úřad pro ochranu osobních údajů],⁶⁸ as well as of various NGOs.⁶⁹ The most current issue is the electronic card (“OpenCard”) issued by the City of Prague, used for public transportation, library access and other services. At the present, the Office for Personal Data Protection is carrying out a control in city institutions offering the “Opencard”; the control is focusing on compliance with legal provisions concerning collection and processing of personal data, as unnecessary collection of personal data, as well as insufficient protection of collected data was suspected.⁷⁰ The “OpenCard” is also a good example of a new negative trend, when level of assured privacy depends on the amount of money data subjects are ready to spend: There are two types of the “OpenCard”, whereas the not personalised, anonymous version is more expensive than the personalised, thus at the end, whether personal data will be collected and stored depends only from the amount the data subject is ready to pay.⁷¹ Upon the request of the authors of this report to the spokesperson of the “OpenCard” project to state reasons for this differentiation, the spokesperson brought forward, that there is a risk of uncontrolled buying and reselling of the

⁶⁸ Cp. Position No. 8/2006 issued by the Office for Personal Data Protection, available at: <http://www.uoou.cz/index.php?l=en&m=left&mid=02:116&u1=&u2=&t=> (in Czech only) (last accessed on 13. January 2009).

⁶⁹ Cp. *Iuridicum Remedium*, Report on the occasion of the European Day of Personal Data Protection (28.01.2008), available at: <http://www.iure.org/656950> (in Czech only) (last accessed on 10. January 2009).

⁷⁰ The Office for Personal Data Protection, Press Release from 10. December 2008 and Press Release from 24. September 2008, available at: <http://www.uoou.cz/index.php?l=cz&m=top&mid=03&u1=&u2=&t=> (in Czech only) (last accessed on 10. January 2009).

⁷¹ Issue of the personalised OpenCard is currently free of charge, issue of anonymous OpenCard costs 200,- CZK; the anonymous OpenCard has been available since 16. December 2008, whereas the personalised since August 2008 already; for further information see: <http://opencard.praha.eu/jnp/en/home/index.html> (in English) (last accessed on 23. January 2009).

anonymous “OpenCard” and the issue fee is considered to be an effective measure against it.⁷²

- [67]. A further activity, which can be considered as endangering effective personal data protection in the Czech Republic, is the overall governmental project “eGovernment”. With this project, the Czech government aims at widening the use of electronic means in public services and administration, such as electronic service (eJustice), in which court proceedings participants can follow the developments in their particular case.⁷³ With the ongoing implementation of this project, authorities and state institutions create and merge databases containing personal data. However, no study or any other documents have been presented yet, which analyze the impact of the project on data protection and the measures to be taken to ensure effective data protection in this context.⁷⁴
- [68]. As considerably harmful, processing and storing of personal data concerning movement of persons and electronic communication can be regarded, such as electronic toll systems on roads, and in particular steadily increasing numbers of camera surveillance systems. Camera surveillance systems are a topic, which has been discussed widely not only by relevant state and non-state institutions, but also in the wide public. The topicality and importance of this issue illustrate not only the numerous complaints received by the Office, but also the activities the Office undertakes in this regard.⁷⁵ At the present, a group consisting of state and non-state actors is discussing the possible solutions as reflection to the fact, that applicable data protection legislation largely neglects this topic. A general consensus has been reached that the current legislation does not provide sufficient basis for dealing with camera surveillance systems and thus legislative changes are necessary. However, it has not been decided yet, whether the existing legislation on personal data protection will be amended, or a special law concerning camera surveillance systems will be prepared.⁷⁶

⁷² E-mail from Mr. Martin Opatrný, the spokesperson of the OpenCard project, received on 30. January 2009.

⁷³ See the webpage of the project, available at: <http://portal.justice.cz/ejustice/> (in Czech only) (last accessed on 10. January 2009).

⁷⁴ Cp. *Iuridicum Remedium*, Report on the occasion of the European Day of Personal Data Protection (28.01.2008), available at: <http://www.iure.org/656950> (in Czech only) (last accessed on 10. January 2009).

⁷⁵ Cp. for example Position No. 1/2008 on installation of camera systems in apartment buildings, available at: <http://www.uouu.cz/index.php?l=en&m=left&mid=02:118&u1=&u2=&t=> (in English) (last accessed on 14. January 2009).

⁷⁶ Interview (09. January 2009) with Mr. František Pospíšil (from the NGO *Iuridicum Remedium*), who participates in the working group. This view has also been expressed in

- [69]. Processing personal data by state authorities, in particular by police and intelligence services becomes increasingly an issue. The Personal Data Protection Act covers this topic only to a small extent; its provisions refer to special laws.⁷⁷ The Office for Personal Data Protection carried out a control in the Department of Criminology, which administers the National Database of DNA. The conclusions of the control were similar to those of the control carried out by the Czech Public Defender of Rights; according to both institutions fundamental rights, as well as personal data protection provisions have been violated e.g. by forcible taking of DNA samples from prisoners.⁷⁸ Even some of the deficiencies have been reduced by the new Police Act⁷⁹, the control carried out by the Office for Personal Data Protection still found failure to comply with laws on personal data protection.⁸⁰
- [70]. Generally speaking, the activities of the Office for Personal Data Protection within the current legal framework can be considered satisfactory. At the present the main deficiency of the Office hampering effective data protection is the weak position in the legislative process. The Office may only comment upon drafts and draft amendments to laws, however, it cannot propose legislation and legislation changes itself.⁸¹
- [71]. Most of the deficiencies in effective data protection are well known to the Office, as well as to other state and non-state actors. There are ongoing preparations for amending the current legislation,⁸² even though no concrete drafts have been presented yet. Broadly speaking, it can be argued, that many of the deficiencies in the Czech Republic are not a matter of better implementation of legislation, but rather a problem of disproportion between new trends in the society and

personal interview on 08. January 2009 with JUDr. Zdeněk Koudelka from the Office for Personal Data Protection.

⁷⁷ Cp. Sec. 3 para. 6 Personal Data Protection Act.

⁷⁸ *The Czech Public Defender of Rights*, Taking DNA samples from prisoners was unlawfull, available at: <http://www.ochrance.cz/dokumenty/dokument.php?back=/cinnost/index.php&doc=1142> (in Czech only) (last accessed on 08. January 2009).

⁷⁹ Czech Republic/ Zákon č. 273/2008 Sb., o policii [Act No 273/2008 Coll., on police], available at: <http://www.policie.cz/ViewFile.aspx?docid=31711&lang=cs> (in Czech only) (last accessed on 10. January 2009).

⁸⁰ Press Release from 10. December 2008, available at: <http://www.uoou.cz/index.php?l=cz&m=top&mid=03:16&u1=&u2=&t=> (In Czech only) (last accessed on 05. January 2009).

⁸¹ Cp. also Chapter 2.

⁸² Personal interview with JUDr. Zdenek Koudelka, the Office for Personal Data Protection, on 08. January 2009.

technology and legal answer to these developments, as for example the problem of PNR data transfer to the USA shows.⁸³

⁸³ PNR data transfer to the USA is a Europe-wide recognized problem. See e.g. Czech *Office for Personal Data Protection*, Press release from 12.09.2007, available at: <http://www.uouu.cz/index.php?l=cz&m=top&mid=03:09&u1=&u2=&t=> (in Czech) (last accessed on 08. January 2009); *European Data Protection Supervisor*, Opinion on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, 20. December 2007, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_EU_PNR_EN.pdf (in English) (last accessed on 09. January 2009).

7. Good practices

- [72]. The Office is an approachable modern state authority available by all means to the general public. Its website, its activities towards the public and its friendly attitude may be seen as a good practice. The Office publishes several publications even though it is not obliged to do that pursuant to the provision of the law (Bulletin, Positions). The Office also gives consultations by the phone and also in person.
- [73]. The Office runs a project aimed at children and youth (“My Privacy! Don’t Watch, Don’t Poke!”) and also an educational program called “Protection of Personal Data in Education” since 2007. These projects help general public to be aware of the rights and obligations arising from the data protection legislation (e.g. one of the issues, the camera surveillance system, was raised by students of the school, where the cameras were installed). The young generation shows its awareness by participation to certain initiatives (e.g. the cameras at school campaign). The Office also cooperated on creation of a TV serial about the data protection in 2006 Unawareness Does Not Excuse – We all Have Secrets (according to the Annual Report of 2006 each episode was seen by approx. 160 000 – 310 000 persons)⁸⁴.
- [74]. Also the practice of electronic forms which can be filled in online may be counted as a good practice, as well as the electronic register of controllers and processor.
- [75]. The financial conditions as an instrument of independence of the Inspectors granted by the Act are worth mentioning.
- [76]. Also very good and detailed Annual Reports are worth mentioning.

⁸⁴ See *Výroční zpráva za rok 2006* (Annual Report of 2006), p. 2 available at http://www.uoou.cz/vz_2006.pdf (accessed on 02.01.2009).

8. Miscellaneous

- [77]. The Office takes part in the activities of the Government Council for Human Rights [Rada vlády pro lidská práva] which is an advisory body of the Government of the Czech Republic on the protection of human rights and fundamental freedoms and of the Government Council for the Information Society [Rada vlády pro informační společnost], which is an advisory body of the Government of the Czech Republic (coordinated by the Ministry of Interior), it deals with the conceptual and coordination questions of the development of the information society and thus partially fulfils the role of the no longer existent Ministry of Informatics.
- [78]. There is also a Standing Commission on Privacy Protection [Stálá komise Senátu pro ochranu soukromí]⁸⁵ in Senate of the CR (the higher chamber of the Parliament of the CR). This commission is a body of the Senate and was established under the Act on the Senate Rules of Procedure [Jednací řád Senátu]⁸⁶. Senate appoints the Commission and the number of Members is the same as the proportional representation of political fractions of the Senate. The Commission cooperates with the Office (respecting its independence) and other central administrative authorities during the legislative negotiations, concerning the privacy of citizens and management of their personal data.

⁸⁵ See http://www.senat.cz/organy/index.php?ke_dni=05.01.2009&O=7&lng=en&par_2=228 (accessed on 02.01.2009).

⁸⁶ Czech Republic/ Act No. 107/1999 Coll. on the Senate Rules of Procedure, as amended (Zákon č. 107/1999 Sb., Jednací řád senátu), Sec. 43 (1).

Annexes

Annex 1 – Tables and Statistics

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority ⁸⁷	1 268 658,84 EUR/ 33 505 280 CZK	2 894 585,38 EUR/ 76 446 000 CZK	2 817 114,72 EUR/ 74 400 000 CZK	3 238 053,76 EUR/ 85 517 000 CZK	7 775 009,46 EUR/ 205 338 000 CZK ⁸⁸	3 498 333,96 EUR/ 92 391 000 CZK	3 613 101,09 EUR/ 95 422 000 CZK	3 516 168,11 EUR/ 92 862 000 CZK
Staff of data protection	11	65	71	70	74	80	89	92

⁸⁷ The figures are available at the website of Ministry of Finance, <http://www.mfcr.cz> (accessed 07.01.2009). The equivalent in Euros is calculated on the basis of the Rate of Exchange published in the Official Journal on 06.01.2009, No. 2009/C 2/07.

⁸⁸ The high budget of the Office of this year (comparing to other years) was appointed because of the purchase of the quarters of the Office to the possession of the state.

authority								
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative							14	
Number of data protection registrations	108	13736	3967	2604	1402	419	945	1195
Number of data protection approval procedures	Not available ⁸⁹ /29	4193/ 322	4301/ 147	2854/ 89	1591/ 52	466/ 684	1195/ 38	1781/ 51
Number of complaints received by data protection authority	40	200	755	264	641	408	476	574

⁸⁹ Number before the slash means the number of requests for registration (given by the data protection subjects), the number beyond the slash is the number of requests for transfer of datas.

Number of complaints upheld by data protection authority	Not available	NA	NA	NA	NA	NA	113	NA
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)	NA	NA	NA 112 (annulled registrations)	NA + 52 (annulled registrations)	NA + 64 (annulled registrations)	NA + 111 (annulled registrations)	64 decisions on penalties in administrative proceedings + 88 penalties for unasked commercial messages (spams) + 92 (annulled registrations)	43 decisions on penalties in administrative proceedings + 71 penalties for unasked commercial messages (spams) + 904

								(annulled registrations)
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)	NA	NA	NA	NA	NA	NA	NA	NA
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)	NA	NA	NA	NA	NA	NA	NA	NA

Annex 2 – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	Personal data processing (including personal identification number) by distrainers
Decision date	16.06.2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	1 As 36/2008-77, Nejvyšší správní soud (1 As 36/2008-77, Supreme Administrative Court)
Key facts of the case (max. 500 chars)	A fine was imposed by the Office for personal data protection ('the Office') on a distrainer, who in preparation of public sale of a distrained property disclosed inter alia the personal identification number of the property owner. This was considered by the Office as a breach of the Data Protection Act No. 101/2000 Coll. The distrainer took legal action against the decision of the Office before the Municipal Court. The Office then appealed then to the Supreme Administrative Court against the decision of the Municipal Court.
Main reasoning/argumentation (max. 500 chars)	The Supreme Administrative Court ('the Court') considered the disclosure to be unlawful. Furthermore it rejected the argumentation of the Municipal Court, which argued that the formulation of Sec. 45/1/c) of the Personal Data Protection Act is vague and thus it is not possible to impose sanctions on the basis of this provision. The Court argued that the wording of Sec. 45/1/c) fulfils all necessary requirements of an administrative offence by stipulating the object, subject, wrongful conduct and damaging consequence.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Supreme Administrative Court clarified two issues. Firstly, distrainers may use personal identification numbers for certain specific purposes, however, in this case the disclosure was a measure exceeding the permitted limits and thus unlawful. Secondly, wording of provisions of the Personal Data Protection Act stipulating the competence of the Office to impose sanctions is precise enough.

Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Supreme Administrative Court remanded the case to the Municipal Court for further proceedings. The main contribution of this case may be seen in the fact that the Supreme Administrative Court confirmed and clarified the characteristics of Sec. 45/1/c) of the Personal Data Protection Act as an administrative offence.
Proposal of key words for data base	Administrative offence – Personal Data Protection Act – processing of personal data – distrainers

Case title	Camera surveillance system in apartment houses
Decision date	28.02.2007
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	7 Ca 204/2005-49 Městský soud v Praze (7 Ca 204/2005-49 Municipal Court in Prague)
Key facts of the case (max. 500 chars)	The complainant lodged an appeal against a fine imposed on him by the Office for personal data protection. The complainant was an owner of an apartment house, in which he installed a camera surveillance system, together with a chip card entry system for the main entrance to that house. The installation was carried out as a reaction of the property owner to frequently occurring damages to the property. As the inhabitants of the house did not consent the installation, the Office considered the installation an offence under Sec. 45/1 Personal Data Protection Act ('Act').
Main reasoning/argumentation (max. 500 chars)	The Court accepted the argumentation of the Office that as there was no consent of the house inhabitants to the collection of data by the system installed, the right to respect for private life was violated, as well as provisions of the Act. Protection of a property as a legitimate interest of the complainant may constitute an exception from the requirement of consenting such data collection, however, in the case of collision of two legitimate interests, protection of right for private life prevails.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Court confirmed the view of the Office that data collected by a surveillance system in an apartment house have to be considered as personal data falling within the scope of the Act. It also confirmed that collection and processing of such data is unlawful if it is not consented by persons affected. Furthermore the Court recalled decisions of the Constitutional Court and the Supreme Administrative Court stipulating the prevailing character of the right to respect for private life in case of a collision with other rights or legitimate interests.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Court dismissed the appeal of the complainant. The use of camera surveillance systems becomes more and more widespread in the Czech Republic, thus also the probability that similar cases will occur is high. This makes the clarification of legal provisions concerning the problem of use of camera surveillance systems, which were touched upon in this case, particularly important.
Proposal of key words for data base	Camera surveillance system – apartment houses – right to respect for private life – definition of personal data

Case title	Competence conflict between the Czech Statistical Office and Office for Personal Data Protection
Decision date	16.01.2002
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	III. ÚS 672/91 Ústavní soud (III. ÚS 672/91, The Czech Constitutional Court)
Key facts of the case (max. 500 chars)	In 2001, the Czech Statistical Office carried out a population census. Following the census, the Office for Personal Data Protection issued a decision on the basis of Sec. 40 of the Personal Data Protection Act ('Act') that certain specific personal data obtained in the census have to be deleted. The Czech Statistical Office considered this decision as going beyond the competence of the Office for Personal Data Protection ('the Office'), refused to delete the data and commenced a competence dispute before the Constitutional Court.

Main reasoning/argumentation (max. 500 chars)	The Constitutional Court denied its competence in this case, as it considered that the competence dispute was inadmissible for following reasons: A competence dispute requires a competence conflict, which means that two authorities claim the competence to issue a decision in the same case; or two authorities refuse to issue a decision, i.e. deny their competence. In this case only the Office issued a decision, and it was entitled to do so as the only authority pursuant to the provisions of the Act.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Constitutional Court, in addition to interpretation of constitutional provisions concerning the competence dispute between authorities, further clarified the position of the Office in relation to the Czech Statistical Office, in particular confirming that the Office is the only authority competent to issue remedy measures under the Act. However, the Court did not go into the merits of the case, i.e. did not consider the lawfulness of the decision as such, issued by the Office.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The proposal to commence competence dispute before the Constitutional Court was dismissed. The Czech Statistical Office, seeking the clarification of lawfulness of the Offices' decision had to lodge an administrative complaint before the competent court.
Proposal of key words for data base	Czech Statistical Office – Office for Personal Data Protection – competence – remedy measures – Personal Data Protection Act

Case title	Securing of Personal Data according to Sec. 13 Personal Data Protection Act
Decision date	10.05.2006

Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	3 As 21/2005 – 105, Nejvyšší správní soud (3 As 21/2005 – 105, Supreme Administrative Court)
Key facts of the case (max. 500 chars)	The Office for Personal Data Protection imposed a fine on the joint company K, as the company did not introduce sufficient measures to ensure protection of personal data of companies' clients, whereas the omission resulted into these client data being stolen. This was considered as a breach of companies' obligation under Sec. 13 of the Personal Data Protection Act ('Act'). K commenced legal action against the imposed fine.
Main reasoning/argumentation (max. 500 chars)	Decisive in this case was <i>inter alia</i> the interpretation of data 'processing' and 'securing'. According to the Court, the Act implements the directive 95/46/EC, and thus it has to be interpreted in the light of the directive. The primary purpose of the directive and that of the Act is to ensure protection of right to privacy, whereas securing data as such is a necessary and somehow 'natural' measure related to the whole data processing. Thus even closely related, these terms are not the same.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Court by recalling some of its previous decisions, as well as decisions of the ECJ, confirmed the duty to interpret provisions of the Personal Data Protection Act in accordance with the relevant EU law, in particular with the directive 95/46/EC. Furthermore it clarified, that the purpose of securing personal data is not securing the data as such, but the protection of right to respect for privacy. The Court also provided clarification of Sec. 13 of the Act, dealing with the duty of the controller to secure personal data.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Court confirmed sanctions imposed on K despite the fact, that after an incident of personal data of clients being stolen, K implemented measures to secure the data, fulfilling therewith its duties under Sec. 13 of the Act.
Proposal of key words for data base	Processing and securing personal data – duty of EU law conform interpretation – protection of right to privacy

Case title	Collection and processing of personal identification numbers and other personal data by libraries
Decision date	22.10.2003
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	7 A 58/2002-40 Nejvyšší správní soud (7 A 58/2002-40, Supreme Administrative Court)
Key facts of the case (max. 500 chars)	The Office for Personal Data Protection carried out a control in the city library of Prague. The Office considered the collection and processing of some of personal data of library clients as not necessary for the given purpose and thus not in accordance with Sec. 5/1/d) of the Personal Data Protection Act ('Act'). The library was ordered to change the library application form used to obtain these data.
Main reasoning/argumentation (max. 500 chars)	The order of the Office to change the library forms so that they comply with the Act is not an infringement of the libraries' ownership rights on books. However, libraries may collect and process personal identification number from their clients, as this number is often the only reliable source of information about a person. Thus the collection and processing of personal identification numbers does not exceed the limits given by the legitimate purpose, to protect libraries' property on books, which the clients did not return.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Office considered the collection of personal identification numbers as going beyond the limits of necessity in order to protect the legal interests of the library. The Court refused this argumentation and ruled that collection and processing of personal identification number by libraries is permissible under the Act. The Court underlined the impact, the Personal Data Protection Act should have in practice; it should inter alia lead to decreasing of the extent of data collection and processing.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The decision of the Office for Personal Data Protection was rescinded and the Office has to issue a new decision in compliance with the judgement. Generally speaking, in the Czech Republic personal identification number is considered to be one of the most important personal data. Cases, however, in which provisions concerning its protection are infringed, are very common, which underlines the importance of this decision.
Proposal of key words for data base	Personal identification number – collection and processing – library – legitimate purpose

Please attach the text of the original decisions in electronic format (including scanned versions as pdf).