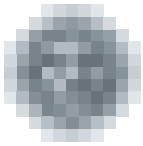


úřad pro ochranu
osobních údajů
the office for personal
data protection

ANNUAL REPORT 2004

Comments of the President of the Office for Personal Data Protection on the Year 2004

While the previous year was the last year of preparation for accession to the European Union, 2004 witnessed a successful climax to these efforts and full membership in EU provided the Office for Personal Data Protection with great potential for international cooperation. The Czech Office was addressed by various governmental and non-governmental organizations concerned with the subject of protection of privacy, and the Office was often invited to make presentations and actively participate at international forums. The Office was also repeatedly requested to give its opinion on international issues of data protection.

While, on the one hand, interest in the state of protection of privacy in the Czech Republic, as a new EU Member State, is gratifying, on the other hand, it also entails considerable obligations. Technical developments and modern technology have practically erased state frontiers in dissemination of information and created new possibilities for encroaching on human privacy. Today, new risks of infringement on privacy are related exclusively to new technologies. Analysis of these risks and, in particular, effective protection of privacy requires both professional expertise and extensive international cooperation. Therefore, without respect to how membership in EU will affect the lives of the citizens of the Czech Republic, it can already be stated that, in the area of personal data protection and protection of privacy, this effect will be positive.

International harmonization of laws is the primary basis for protection of privacy. The regulations of EU and of the Council of Europe are globally respected legal instruments. Not only European countries, but also a number of states from other parts of the world, strive to ensure harmonization with these regulations. The Czech Personal Data Protection Act was also amended in 2004, with a view of its full harmonization with the EU laws. This brief statement encompasses considerable work and efforts of the Office for Personal Data Protection.

Furthermore, the Office has become a respected institution, whose opinions, comments and ideas are becoming increasingly incorporated into the relevant regulations. This is a good sign and it can be assumed that personal data protection will be enshrined in the Czech legislation in accordance with European legal principles.

Organization of an international conference of the Council of Europe entitled "Rights and Responsibilities of Data Subjects" was the most important international activity of the Office in 2004. The fact that the Council of Europe entrusted the Office with organizing the conference in Prague reflects its confidence in the quality of the work of this Czech institution.

Currently, the Office is no longer in a position where it would require assistance from the Council of Europe or EU, but is rather becoming an active cooperating institution and can offer and provide its own assistance to countries, where personal data protection has not yet attained a suitable level. An important act in this relation consisted in the submission of a joint Czech-Spanish proposal for as-

sistance in incorporating personal data protection in the legal and institutional environment of Bosnia and Herzegovina. Through this proposal, the Office applied for a twinning project of the European Commission, for the first time, as a provider, rather than a beneficiary. The Czech-Spanish proposal is currently being assessed by the Delegation of the European Commission in Sarajevo. A decision should be made in early 2005.

Further competence was entrusted to the Office in 2004. Amendment to the Act on Register of Population and Birth Numbers imposed on the Office supervisory duties in the area of management of birth numbers. Certain Information Society Services Act introduced new duties in the sphere of dissemination of commercial communications. The aforementioned new competence, not only results in a substantial increase in the workload, but also imposes new requirements on human resources. Negotiations with the Government of the Czech Republic next year will be concerned with an increase in the personnel of the Office.

The Office constantly strives to raise the awareness of the citizens of their rights in relation to the protection of privacy. A well-informed citizen can often defend himself against unauthorized infringement on his privacy. Indeed, the efforts of the Office to provide the required information have led to favourable results, not only in relation to the number of complaints, but also with respect to the various enquiries. In late 2004, we finished the preparation of the first information leaflet, which will be distributed to citizens through regional, city and municipal offices at the beginning of 2005. These activities of the Office will be continued next year.

Nevertheless, awareness activities will also need to concentrate on controllers and processors of personal data. The fact that a number of institutions, both public and private, know almost nothing about protection of privacy and protection of personal data was again confirmed in 2004. Some cases of processing of personal data, are beyond comprehension. The Office encounters, not only ignorance of legal issues, but often also arrogant refusal to respect the right of citizens to privacy, intentional evasion of the Personal Data Protection Act and dishonest efforts to enforce legislative changes in laws that would permit processing of personal data at variance with democratic principles. Especially certain areas cause concerns and fears of dangerous infringement on the privacy of individuals from the viewpoint of protection of their personal data.

Respect for privacy and combating national and international terrorism

Since 2001, the fight against international terrorism has changed views on the protection of privacy. In numerous cases, measures infringing on the right to privacy were justified by the need to combat terrorism. However, these measures are often not accompanied by analysis of the particular benefits. It has shown, also in international context, that the need to combat terrorism has become an excuse for implementing measures that have no clear effect. A number of critical standpoints were presented at the end of the year, particularly by some members of the European Parliament, noting the creeping effect of breach of privacy. However, the opinion that the fight against terrorism is a sufficient reason for any measure whatsoever, which cannot be subject to discussion and balanced by protection of privacy of citizens, still prevails in the Czech Republic. Particularly in relation to attempts to create further records, to extend the rights to access personal data and to obtain personal data from the existing records, and to extend the duty to disclose identification in situations, where anonymity has been granted to date, and in relation to the pressure for increasing the scope of data during identification – under all the above circumstances, a statutory basis will always be required and analysis will have to be presented, demonstrating the effectiveness of such measures.

Telecommunications

Discussions began in late 2004 on an issue that is of concern to a number of EU countries. The telecommunications sector has instruments that are amongst the greatest instruments of infringement of the privacy of citizens. Tapping of telephone lines, storage of "transaction data", lease of telephone lines for pursuing illegal activities, excessive collection of personal data and copying of personal documents of the users of telephone networks, sending unsolicited commercial communications to users – these are the most pressing issues that must be addressed especially from a legislative viewpoint.

Camera systems

I drew attention to this issue in last year's annual report in relation to school facilities. The use of camera systems was further extended in 2004 in both the public and private sectors. The number of cameras installed on public premises is constantly increasing, without at least basic legal rules being adopted in this respect. Nobody controls whether the cameras installed in public areas infringe on human privacy, e.g. by simultaneous recording (or permitting recording) of premises that are not public. There are no set rules for the use, keeping and deleting recordings. Camera systems are being increasingly installed on premises where individuals should have the right to privacy. Issues related to monitoring employees at workplaces will also become more frequent. The Office commenced the first control in this area in 2004; however, this control has not been completed to date.

Land registry and other publicly accessible registers

Inadequate understanding of the purpose of publicly accessible records and registers came to light in some cases in 2004. Personal data from publicly accessible registers (e.g. the land registry) were used for purposes other than those for which they were collected in the registers. This demonstrated that it is difficult to convince the administrators of these registers to restrict the provision of personal data. Apparently, it will be necessary to request that legislative measures be adopted to prevent misuse of personal data from publicly accessible records.

New technologies – RFID, biometric data

New technologies, particularly in the area of computing and communications, create new risks for the privacy of citizens. These new technologies provide new potential for processing information, including personal data, create new types of personal data (e.g. transaction, contact, localization, etc.) and permit storage of increasing amounts of information on electronic memory media. This progress gradually creates a potential for recording all the activities of each person during his or her life (Bruce Schneider calls this "individual life recording v _eské verzi je: recorder"). The current capacity of computer memories already permits, e.g., recording of all the words uttered by a person speaking 8 hours a day and living for 80 years, during his or her entire life.New technologies will require due attention. Disputes will inevitably occur between those who advocate protection of privacy and producers and distributors as to the necessary scope of legal limitation of technologies endangering privacy of citizens.

Unsolicited commercial communications, spam

Directive 2002/58/EC of the European Parliament and of the Council substantially affected the area of marketing, introducing especially regulation of electronic communications. Expectations that implementation of this Directive in the Czech legislation would substantially reduce the massive inflow of unsolicited e-mails, i.e. spams, have not been fulfilled. This has shown that prevention of spamming through

legal regulations is not very effective. In addition to software and technical tools, it is also necessary to promote proper behavior of users of the Internet.

Health care, social sector

In all of Europe, health care and social care belong amongst the most problematic sectors from the viewpoint of processing of personal data. While the use of identification data from the national health-care registers was restricted in 2004, a new issue arose in connection with "medical certificates". Certain proposed forms of this certificate encompass great risks of misuse of medical data. Introduction of electronic technology in health care has been very slow, which, given the vast amounts of processed personal data (furthermore, usually sensitive data), leads to justified concerns from the viewpoint of protection of the private lives of citizens.

Self-government, public sector

The Office has repeatedly encountered substantial ignorance of the legislation, including the Personal Data Protection Act, in various areas of government. This ignorance often results in unwillingness to change the most straightforward, long valid or obsolete procedures, which, however, diminish respect for privacy and the right of citizens to its protection. Ignorance of the basic principles of protection of personal data causes considerable problems for citizens, who have inadequate means of defending themselves. Similar to the previously encountered issue of unauthorized disclosure of lists of debtors, in 2004, we repeatedly dealt with, e.g., publication on the Internet of minutes of meetings of municipal assemblies and city and municipal councils containing the personal data of citizens. Although the Office has issued an explanatory position on this issue and disseminated this position at all levels of self-government, it has frequently encountered lack of understanding by the officers and has been repeatedly accused of restricting access of citizens to information. Application of the "balance principle", where a balance needs to be established between the interests of authorities and the interests of citizens, causes problems to a number of officials.

RNDr. Karel Neuwirt

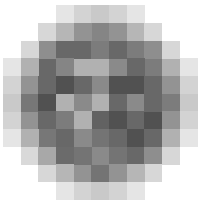
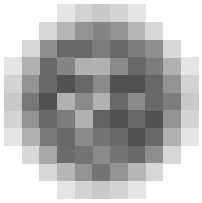


Table of Contents



Activities of the Office in Numbers – 2004

Enquiries	E-mail enquiries	975
	Enquiries received by mail – legal persons	261
	Enquiries received by mail – natural persons	96
	Telephone enquiries	5 207*
Complaints**		335 + 306***
Control activities	Total number of controls	79
	completed	71
	according to the plan	19
	incidental controls	60
Administrative punishment	Total instigations received	45
	Decisions on imposing a fine	35
Registration	Total number of controllers	21 709
	Total number of cases of processing registered	24 588
	Total number of notifications in 2004	1 972
	Number of applications concerning transborder transfer of personal data (Article 27 of Act No. 101/2000 Coll.)	52
	Number of permitted transfers	35
Commented legislative drafts	Acts	72
	Decrees	107
	Regulations of the Government	36
	Other	80
Institutions on whose materials (not only of legislative nature) comments were provided	Czech National Bank	1
	Czech Mining Authority	1
	Czech Geodetic and Cadastral Office	4
	Czech Statistical Office	1
	Office for the Protection of Competition	1
	Administration of the State Material Reserves	1
	State Office for Nuclear Safety	1

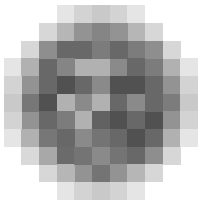
	Industrial Property Office	1
	Office of the Government	11
	Ministry of Informatics	14
	Ministry of Environment	34
	Ministry of Labor and Social Affairs	20
	Ministry of Transport and Communications	15
	Ministry of Interior	29
	Ministry of Defense	4
	Ministry of Foreign Affairs	10
	Minister of Education, Youth and Sports	26
	Ministry of Justice	25
	Ministry of Health	56
	Ministry of Finance	15
	Ministry for Regional Development	15
	Ministry of Culture	2
	Ministry of Industry and Trade	9
	Ombudsman	1
Personal consultations	Consultations provided to citizens and institutions	89
Lectures, seminars	(active presentations)	33
Materials published	Journal of the Office (number of editions)	6
	Bulletin of the Office (number of editions)	4
	Positions / "On practical issues"	7
	Translations of foreign documents	10
	Press releases and communications for the press	26
	Additional basic documents for media	66
Press conferences	Regular press conferences of the Office	4
	Extraordinary	1
Contact with the media	Agency service, press, radio and television	354

** Including, with accuracy of the order of tens, only outputs from workplaces providing special answers by telephone.*

*** Including instigations sent directly to the Office as complaints*

**** Number of accepted complaints against unsolicited commercial communications from the date of effect of Act No. 480/2004 Coll., on Certain Information Society Services and on the Amendment to Certain Other Acts (i.e. for the period from September 7 to December 31, 2004)*

(The table depicts the state of affairs as of December 31, 2004.)



Control and Supervisory Activities of the Office

FINDINGS AND OUTPUTS OF CONTROLS PERFORMED BY INSPECTORS OF THE OFFICE

Control activities of the Office were carried out in 2004, not only according to the control plan, but particularly on the basis of instigations and complaints. The controls were directed and performed by inspectors. Certain controls also involved other employees of the Office.

Inspectors pursued 79 controls in 2004. Of this number, 19 controls were initiated on the basis of the control plan and 60 controls were performed on the basis of complaints and instigations. 71 controls were completed during the relevant year, of which 12 controls were initiated in the previous year and 8 controls have not been validly completed due to the objections raised both in the first and in the second, appellate, instances. Controls initiated pursuant to the control plan were usually conceived as comprehensive controls, i.e. the review covered all the duties prescribed by the law for controllers and processors in processing of personal data. The control plan in 2004 was concerned particularly with the area of education, information systems of the Police of the Czech Republic, processing of personal data by cities and city wards and selected corporations. The substantial amendments to some laws introduced in 2004, which were important for assessing the duties of controllers and processors, also influenced the assessment of ascertained facts, mainly with respect to the legal force of the amendments.

The range of controlled entities was again very broad. Inspectors commenced controls, not only on the basis of complaints submitted to the Office, but also in response to instigations in the media, which initiated approximately 20 percent of cases. These cases involved, for example, finding of parts or even entire files, leaking of personal data, camera systems, unauthorized publication of personal data and misuse of records for other than specified purposes. The control was concerned with both minor controllers and processors – individuals and small companies, including providers of internet connections, civic associations, associations of breeders, housing cooperatives, associations of owners of buildings, etc., and major governmental processors of personal data, such as the ministries, police, prison administration, city and municipal authorities. Control was also aimed at processing of personal data at universities, secondary and elementary schools, in hospitals, publishing houses, employment and marriage agencies and professional chambers, and in the area of transport. Controls of banks, insurance companies and other financial institutions were commenced and further pursued during the relevant year. The range of controlled entities also included hypermarkets, commercial companies, administrators of distribution networks and detective agencies.

Inspections usually revealed breach of several duties imposed on the controllers and processors by the Personal Data Protection Act. Violation of the Act was ascertained in almost 60 % of the controlled entities. Liquidation of personal data was imposed in seven cases. The increasing number of cases, where shortcomings were already remedied by the controllers during the control and, there-

fore, no remedial measures had to be imposed, is a positive feature. These cases involved mainly minor shortcomings in the processing of personal data. During controls, the inspectors also pointed out the changes and new duties of controllers following from amendments to other laws, particularly the Act on Register of Population and Birth Numbers and the Act on Identity Cards and Travel Documents.

The experience of the inspectors shows that, in addition to incidental controls, attention must be further paid in creation of the control plan to major processors of personal data, whose processing fundamentally affects the privacy of citizens. Breach of duties in processing of personal data is also regularly found during these controls, both from the viewpoint of the scope of processing of personal data and from the viewpoint of the manner of collecting and handling thereof.

Recognition through photographs as an issue of personal data protection

I. M. and R. Ch. lodged a joint action with the District Court in C. Through this action, dated May 12, 2000, the plaintiff, R. Ch., claimed that the court impose on the Czech Republic – the Ministry of Interior – the duty to refrain from conduct aimed at inclusion of a photograph of the plaintiff, together with his name, surname and date of birth, in the file kept by the Police of the Czech Republic – the District Bureau of Investigation in C. – and later by the District Court in C., and that a duty be imposed to remove the photograph, including the above-mentioned personal data, from the picture album kept by the District Bureau of Investigation in C. and to destroy the photograph and personal data of the plaintiff. Through Resolution of the Supreme Administrative Court in Brno of March 10, 2004, Ref. No. Konf 11/2003-12, it was ruled that the competence to make a decision on the petition lay with the Office for Personal Data Protection (hereinafter the "Office").

Similarly, before the same court, plaintiff I.M. claimed that conduct aimed at inclusion of a photograph of the plaintiff, together with his name, surname and date of birth, in the file kept by the Police of the Czech Republic – the District Bureau of Investigation in C. – and later by the District Court in C., be refrained from and that a duty be imposed to remove the photograph, including the above-mentioned personal data, from the picture album kept by the District Bureau of Investigation in C. and to destroy the photograph and personal data of the plaintiff. In this case, it was again ruled, through Resolution of the Supreme Administrative Court in Brno of February 6, 2004, Ref. No. Konf 15/2003-24, that the competence to make a decision on the petition lay with the Office.

Therefore, it was necessary to ascertain through control, how Department X of the Police of the Czech Republic and the District Directorate in C. process personal data for the purpose of recognition through photographs and whether they violate the Personal Data Protection Act in their processing of personal data for recognition through photographs. In accordance with the competence of the Office, the control could be concerned only with such conduct of the controlled departments of the Police of the Czech Republic that corresponded to the definition of processing of personal data pursuant to the Personal Data Protection Act.

The provisions of the following laws were used as a legal framework for fulfillment of the duties of the Police of the Czech Republic pursuant to the Personal Data Protection Act:

- Act No. 141/1961 Coll., on criminal court proceedings (the Code of Criminal Procedure), as amended (hereinafter the "Code of Criminal Procedure");
- Act No. 283/1991 Coll., on the Police of the Czech Republic, as amended (hereinafter the "Act on the Police of the Czech Republic");

- Constitutional Act No. 1/1993 Coll., the Constitution of the Czech Republic, as amended;
- Act No. 328/1999 Coll., on identity cards, as amended (hereinafter the "Identity Cards Act");
- Act No. 133/2000 Coll., on Register of Population and Birth Numbers and on Amendment to Some Laws, as amended (Register of Population Act);

and also the following regulations:,

- Resolution of the Presidium of the Czech National Council of December 16, 1992 on promulgation of the Charter of Fundamental Rights and Freedoms as part of the constitutional order of the Czech Republic No. 2/1993 Coll., as amended by Constitutional Act No. 162/1998 Coll., and
- Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, promulgated under No. 115/2001 Coll. of Int. Treaties (hereinafter "Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data").

Account was also taken of Award of the Constitutional Court III. ÚS 256/01 (Coll. of Awards of CC, 2002, Volume No. 25, Award No. 37) on recognition through photographs, Resolution of the Constitutional Court IV. ÚS 143/02 of August 28, 2002, and Recommendation No. R(87)15 of the Council of Ministers for the Member States of the Council of Europe providing for use of personal data in the police sector.

The above-cited regulations, as a whole, were taken into account as a basis for decision-making. Articles 5 (3), 10, 13 (1) and 22 were used as a basis for assessing the potential violation of the Personal Data Protection Act. Furthermore, Article 3 (6) (d) was also relevant in this respect. The provisions of the Personal Data Protection Act were taken into account both in the wording valid on the date of commencement of the control and in the wording valid on the date of completion of the control. The relevant provisions of Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, i.e. Articles 5, 7, 8 and 9, and Recommendation No. R(87)15 of the Council of Ministers for the Member States of the Council of Europe providing for use of personal data in the police sector, together with the provisions of Titles Four and Five of the Act on the Police of the Czech Republic, were also taken into account.

All the handling of the personal data of the plaintiffs by the Police of the Czech Republic, which was contested by the actions, took place prior to the date of effect of the Personal Data Protection Act. Therefore, the handling could not be subject to control pursuant to the Personal Data Protection Act. At the time of recognition through photographs, which was the subject of the actions, the Police of the Czech Republic employed the procedure described in Award of the Constitutional Court III. ÚS 256/01 (Coll. of Awards of CC, 2002, Volume No. 25, Award No. 37) on recognition through photographs. The control was concerned with handling of personal data for the purposes of recognition through photographs undertaken by the Police of the Czech Republic in 2003 and 2004.

It was ascertained that the Police of the Czech Republic performs acts for the purposes of recognition through photographs usually ad hoc, exclusively in the framework of a single file. At the time of performance of the control, the Police of the Czech Republic used, for the purposes of selecting persons for recognition through photographs, exclusively personal data available through remote access in the information system, in which the Ministry of Interior kept, under various laws, inter alia, personal data from the register of population and data from the records of identity cards, including identity-card photographs.

The Police of the Czech Republic performs a set of operations with the personal data for recognition through photographs, comprising search for photographs and identification and contact details in the records of identity cards, and printing and use thereof, including graphic modification of the photographs and inclusion of the photographs, together with identification and contact details, in picture albums and, within the albums, in the criminal files. Another set of operations consists of recording the name, surname and full date of birth in the protocol of recognition and use of photographs and identification data for recognition. Operations involving personal data are performed in the framework of individual cases.

All operations are performed within the fulfillment of tasks of the Police of the Czech Republic in detection of criminal offenses and identification of offenders and in investigation of criminal offenses, i.e. to carry out tasks imposed on the Police by Article 2 (1) (d) of the Act on the Police of the Czech Republic and the provisions of the Criminal Code.

In the individual cases, the set of operations performed by the bodies of the Police of the Czech Republic with personal data from the records of identity cards for the purposes of recognition through photographs does not constitute processing of personal data pursuant to the Personal Data Protection Act. The defining features of processing of personal data pursuant to Article 4 (e) of the Personal Data Protection Act are met by the set of operations performed by the Police of the Czech Republic, as armed security corps of the Czech Republic, fulfilling tasks in matters of public policy and safety, and other tasks within the scope and in the manner stipulated by the legal regulations, in relation to personal data from the records of identity cards for the purposes of recognition through photographs in general, as these activities comprise the same repeated operations with personal data from the records of identity cards.

Therefore, the procedure of the bodies of the Police of the Czech Republic in preparation, implementation and documentation of recognition through photographs is subject to the regime established by the Personal Data Protection Act only to the extent of use of the records of identity cards as a source of personal data and photographs, i.e. to the extent delimited by search for (selection) of photographs and other personal data and their withdrawal from the original data file and incorporation in another, newly created file including personal data in the form of a pictorial document. Responsibility for such processing is borne by the departments of the Police of the Czech Republic that pursue personal data processing to that end.

The Police of the Czech Republic fulfill tasks imposed explicitly on them by the Act on the Police of the Czech Republic. As a body of public power, the Police of the Czech Republic is subject to the Personal Data Protection Act, with exemptions stipulated in Article 3 (6) (d) of the Personal Data Protection Act and with a special regulation encompassed in the Act on the Police of the Czech Republic and the Code of Criminal Procedure. An exemption from the duties pursuant to Article 5 (1) and Articles 11 and 12 applies to processing of personal data for the purposes of recognition through photographs.

The instigation and control findings did not indicate the need to deal with any explicit right of the affected data subjects, i.e. the plaintiffs, I.M. and R. Ch., as stipulated by the Personal Data Protection Act as of the date of completion of the control. However, it was necessary to ascertain whether the processing of personal data for the purposes of recognition through photographs involves any infringement on the right to protection of private and personal life of the data subject. This is a duty following for the controller from Article 5 (3) of the Personal Data Protection Act.

Processing of personal data from the records of identity cards for the purposes of recognition through photographs does not infringe on the rights of data subjects, whose personal data recorded in the records of identity cards are processed for the purposes of recognition through photographs, as follows from Award of the Constitutional Court III. ÚS 256/01 (Coll. of Awards of CC, 2002, Volume No. 25, Award No. 37). There is also no infringement on the private and personal life of data subjects, which is an interest explicitly protected by the Personal Data Protection Act.

Until July 26, 2004, processing of personal data for the purposes of recognition through photographs was subject to Article 22 of the Personal Data Protection Act. According to the above-cited provision, the data subjects, i.e. plaintiffs I. M. and R. Ch., were not entitled to request that the Police of the Czech Republic liquidate personal data after the Personal Data Protection Act came into effect.

In processing of personal data from the records of identity cards for the purposes of recognition through photographs, the controlled departments of the Police of the Czech Republic should ensure protection of the private and personal lives of the data subjects. Pursuant to the wording of the Personal Data Protection Act valid as of July 26, 2004, the duty to ensure protection of the private and personal lives of the data subjects is borne by the controlled departments of the Police of the Czech Republic pursuant to Article 5 (3) of the Personal Data Protection Act, as they perform the processing on the basis of a special law. A similar duty pursuant to Article 10 of the Personal Data Protection Act was applicable until the aforementioned date. The processing of personal data, which was ascertained during control, was assessed as a process proposed and implemented in a manner not resulting in breach of the duties of the controlled departments of the Police of the Czech Republic to ensure protection of the private and personal lives of data subjects.

A standpoint included in Award of the Constitutional Court III. ÚS 256/01 (Coll. of Awards of CC, 2002, Volume No. 25, Award No. 37) on recognition through photographs was taken as decisive with respect to the alleged infringement on the rights of the data subject pursuant to Article 10 of the Personal Data Protection Act. The controlled entity did not breach its duty pursuant to Article 5 (3) of the Personal Data Protection Act and, prior to July 26, 2004, it did not breach the corresponding duty pursuant to Article 10 of the Personal Data Protection Act.

It follows from the petition that the relevant right of the plaintiffs, I. M. and R. Ch., consists in the right pursuant to Article 8 (a) of Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, i.e. the right to obtain information on the existence of an automated set of personal data, its main purposes, as well as the identity and usual seat or main workplace of the controller of the set of data.

This right could not have been infringed with respect to organization of the processing, comprising use of an automated set of personal data, whose existence can be ascertained by the affected data subject from the law regulating the records of identity cards. Nevertheless, the wording of the provisions of the Personal Data Protection Act, assessed together with Article 47a (2) of the Act on the Police of the Czech Republic, does not correspond to the purpose that is to be achieved through the relevant right. The data subject cannot assume or deduce that his photograph and other personal data have been processed for the purpose of recognition through photographs on the basis of the statutory provision, and that the Police of the Czech Republic is entitled to request, within the fulfillment of its tasks and within the scope required for fulfillment of a specific task, that the relevant controller or processor provide it with information from the records of identity cards in a manner allowing for remote and continuous access. In this

case, the effect contemplated by Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data is not achieved.

Thus, the statutory regulation used by the Police of the Czech Republic in processing of personal data from the records of identity cards for the purposes of recognition through photographs and in other handling of personal data during control does not meet the requirements of Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data in relation to guarantees for the data subject, which the Czech Republic is committed to respect.

The provisions of Recommendation No. R(87)15 of the Council of Ministers for the Member States of the Council of Europe providing for use of personal data in the police sector should be used with respect to the fact that, on the basis of ratification of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) regarding supervisory authorities and transborder data flows across the borders of the Czech Republic on September 24, 2003, the provisions of Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data also apply to non-automated processing of personal data.

Given this fact, the legal regulation of personal data processing in connection with and for the purposes of recognition through photographs is not in accord with Recommendation No. R(87)15 of the Council of Ministers for the Member States of the Council of Europe providing for the use of personal data in the police sector, in that it does not meet the requirements stipulated in principle 2.2 and principles 6.1 and 6.4.

The fact that data on an individual have been collected and maintained without his knowledge and have not been deleted gives effect to the conditions for application of the second procedure, i.e. that the data subject should be notified that information is kept thereon, as soon as the purpose of these activities can no longer be assumed. Simultaneously, this condition should be subjected to principle 6 (4), according to which the exercising of the right to access, correction and liquidation of data should be limited only if the limitation is required for the performance of the statutory duties of the police or if it is necessary for protection of the data subject or the rights and freedoms of others. No parts or assumptions of this condition are met in processing of personal data for recognition through photographs.

The control of processing of personal data from the records of identity cards for recognition through photographs performed by the Police of the Czech Republic did not ascertain any breach of the duties imposed on the Police by the Personal Data Protection Act or the duties imposed by the Personal Data Protection Act on the employees of the controlled entity.

It follows from the documentation provided by the court and either submitted by the controlled entity or acquired by the controlling entity that the procedures employed by the Police of the Czech Republic in processing of personal data for the purposes of recognition through photographs are in full accord with the valid laws binding the Police of the Czech Republic and fall within the limits of these laws. However, they do not correspond to the principles and rules of protection of personal data, to which the Czech Republic agreed by ratifying Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) regarding supervisory authorities and transborder data flows and that apply both within the jurisdiction of the members of the Council of Europe and in the Member States of the European Union. The relevant procedures are also not in accord with the requirements

imposed on the legal regulation of personal data processing in the European Union; these requirements are encompassed in Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and in the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS) regarding supervisory authorities and transborder data flows, and also in Recommendation No. R(87)15 of the Council of Ministers for the Member States of the Council of Europe providing for the use of personal data in the police sector.

This legal state affects the position of a data subject and his right to access information on personal data processed on the data subject.

Banking sector

The trend of contracting debts by households continued in 2004, particularly through consumer loans. At the end of the year, approximately every third household had outstanding loans, with the total amount of the debts exceeding CZK 300 billion. This trend was greatly supported by the banking sector, as the degree of risk associated with classified loans increased to almost ten percent, which is very favorable for the banks.

In the competition to obtain the greatest share in this lucrative market segment, which is by no means as saturated as in more developed countries (e.g., in Europe, approx. 50 % and, in the U.S. and Great Britain, almost 70 % of households have outstanding debts), and in order to reduce the costs of advertising campaigns, some banks also employed methods encompassing violation of the Personal Data Protection Act. The well-known case of a bank, which forced its employees to furnish the employer with contact details and more detailed information on their relatives and friends, who were then internally evaluated and contacted by agents with an offer of products of the bank, is an example. Control performed by the Office then revealed that, in its internal instructions, the bank entirely neglected the statutory duty to request approval and notification obligations and it also failed to advise its employees of these statutory duties. Of course, the violation of the Personal Data Protection Act was penalized. The trend of requesting "consent" to activities that are not regulated by laws concerning the banking sector and the financial sector in general continued from 2003. By this "consent", banks, leasing companies, credit companies, etc. allow for disclosure of the financial history of their clients, to a various extent and in varying quality. Simultaneously, it must be admitted that especially banks are forced to this degradation of freedom and of the seriousness of consent as a legal act (see Article 34 et seq. of the Civil Code) by their regulatory bodies, the conclusions of conferences, such as Basel II, and particularly lack of clear statutory rules for exchange of information on clients between banks and other entities pursuing business activities in the area of finance. The idea that a several-year financial history of a client, which is subject to bank secrecy, is obtained and is to be professionally evaluated by employees of various companies lending money, must be depressing and socially degrading for citizens, not to mention the great risk of leakage of personal data on the financial history and standing of the client. According to information available to the Office, the situation where such "consents" are coerced under the threat of not providing a service is becoming more and more frequent and the Office intends to address this issue. However,, as mentioned in the Annual Report of the Office for 2003, the main issue is the lack of statutory rules, such as the rules guaranteed by SCHUFA in Germany or the Credit Report in the U.S.

A number of complaints in 2004 were concerned with copying of personal documents. The year 2004 was complex from the viewpoint of both the Office and the banks, as a number of essential laws were amended, such as the Personal Data

Protection Act, Act No. 328/1999 Coll., on identity cards, Act No. 133/2000 Coll., on Register of Population and Birth Numbers, and Act No. 61/1996 Coll., on certain measures against legalization of proceeds from crime. The amendments to the above-cited laws had a fundamental effect on the discussed issues, which required changes in the approach of the Office to the performance of supervisory activities. In order to provide some indication on the procedure of the Office in the performance of supervisory activities, Position No. 6/2004 (Copying of personal documents from the viewpoint of the Personal Data Protection Act) was published in Journal of the Office No. 35/2004, which should facilitate a change in the manner of processing of personal data by the entities processing such data.

Health Care

Inspections of health-care facilities continued in 2004. Compared to 2003, when the state of protection of personal data was controlled particularly in small hospitals, the priority for 2004 consisted in reviewing the state of securing the personal data of patients in large health-care facilities (hospitals with regional competence, faculty hospitals).

It can be stated with satisfaction that the level of securing personal data by the controlled entities is very good. The relevant binding internal regulations stipulating the ways and forms of protection of data and, thus, also the personal data of patients are usually in place and maintained. There has also been a certain favorable shift (compared to previous years) in the understanding by the health-care facilities of the need for protection of personal data. It is arguable whether this fact was caused by consistent awareness-raising by the Office or whether certain criminal cases (e.g. medical documentation of athletes found in a forest in the Jablonec region, finding plans of operations near waste bins, etc.) have provided the necessary deterring incentive. However, consequently, the ways and forms of personal data protection have improved, which can be demonstrated, e.g., by the consistent updating of the applicable internal regulations of health-care facilities in response to amendments to legal regulations, development of information technologies, etc.

A favorable result has also been achieved in dealing with the issue of providing data to the national health-care registers. As stated in the Annual Report for 2003, health-care facilities submitted the personal data of patients to the national health-care registers in a manner contrary to the law. A change in the legal state occurred on April 9, 2004, i.e. on the date of effect of Act No. 156/2004 Coll., which appropriately amended the Act on Care for the Health of the Population. Disputable Decree of the Ministry of Health No. 470/2003 Coll. was also repealed, namely by Decree No. 552/2004 Coll. of October 20, 2004, on submission of personal and other data to the National Health-Care Information System for the needs of keeping national health-care registers. At the end of 2004, it can thus be stated that, where the personal data of patients are provided by health-care facilities to the national health-care registers, this is carried out on the basis of the applicable law and its implementing regulations and without fault from the viewpoint of the Personal Data Protection Act.

Social affairs

The inspectors received complaints from the workers of open facilities for drug users that they are forced to not secure the anonymity of their clients. In order to provide a brief explanation of this issue, it must be stated that the basic preconditions for the activities of open facilities (usually contact centers, i.e. "C-centers") include free admission, no charge and guaranteed anonymity of the clients. Indeed, anonymity of the clients is absolutely fundamental for the activities and

purpose of C-centers, as a vast majority of the clients visit such facilities only under the precondition that they will never be identified by anyone.

Inspection was carried out in an important organization operating a network of C-centers. Supplementary inspections were performed in some other organizations on the basis of the ascertained facts and, therefore, the final results provide a general picture of the actual state of affairs in the entire Czech Republic.

It was ascertained that C-centers in the Czech Republic receive specific data from their clients, concerning, not only their more detailed identification, but also detailed medical and other data on their drug addiction. The identification details are sufficiently unique to enable finding a specific client in any C-center in the Czech Republic (e.g. to monitor the treatment of a migrating client, elimination of duplicities, etc.), however, without the possibility of his identification. Therefore, it can be ascertained that a specific, unambiguously described person underwent therapy at a certain time and at a certain place; however, this person cannot be identified. Thus, the processed data are anonymous from the viewpoint of the C-centers. C-centers further process these data through an electronic database, which is common for all facilities; therefore, all C-centers have the same data on their clients. This electronic database is guaranteed and administered by the National Monitoring Center for Drugs and Drug Addictions of the Office of the Government of the Czech Republic. All C-centers submit data on their clients, generated from the above-mentioned electronic database, to the National Monitoring Center. Data are submitted in an aggregated form and absolutely anonymously, and serve for monitoring of illegal drugs and preparation and implementation of procedures within the fight against illegal drugs.

However, the above-mentioned electronic database of C-centers is also used for other purposes. Such voluntary "by-products" generated by C-centers include regular sending of print-outs from the database to the bodies of the hygiene service. These print-outs are generated by the database and each individual client is described in the print-out by means of a code, which is structured as follows: the first 6 characters of the birth number of the client (i.e. 6 digits of the birth number before the slash, including automatic adding of 50 to the number of the month for women), slash, the first 3 letters of the first name of the client, identification of the sex of the client and numeral designation of the region and district of the place of residence of the client (in Prague, designation of the city ward). Given the above-described contents and form of print-outs and given the ability of the bodies of the hygiene service to identify a majority of the clients through comparison with other databases, including non-public databases (bodies of the hygiene service have, e.g., the statutory entitlement to access the information system of register of population), this procedure involves processing of personal data in the sense of the Personal Data Protection Act. However, processing of personal data is not essential in this case, as the bodies of the hygiene service (as has been ascertained) do not require the personal data of the clients, but rather only aggregated data for statistical processing. Arguments of the hygiene officers as to why they need to identify the clients through the above-described code, were arbitrary, as they stated that such a code merely facilitates the search for a client.

On the basis of the above-described findings, it was recommended that the National Monitoring Center change the software of the electronic database of C-centers so that the print-outs intended for the bodies of the hygiene service do not include data, through which clients could be identified. The director of the National Monitoring Center confirmed that he would respect the recommendation of the office, that the relevant software would be modified and that the required anonymity of clients would thus be ensured.

Personal data of students, employees, and persons applying for study or employment

Controls of processing of personal data of students and applicants for study, carried out at universities and secondary schools, and controls of employers in relation to the personal data of employees and applicants for employment, yielded some fundamental general findings from the viewpoint of the duties imposed by the law.

Applicants for study must fill out Applications for Study, whose forms are stipulated by the Ministry of Education, Youth and Sports of the Czech Republic (hereinafter the "Ministry of Education") and which must be compulsorily used by secondary schools; they are only recommended for universities. Although there have been a number of changes in these questionnaires, compared to past times, when the activities of parents could affect the acceptance of a student for study (questions concerning parents are no longer included), they continue to contain information that is not required for the given purpose, i.e. decision-making on acceptance or non-acceptance for study. Indeed, Article 5 (1) (d) of the Personal Data Protection Act clearly stipulates that "the controller shall be obliged to collect personal data corresponding exclusively to the specified purpose and in an extent that is necessary for fulfillment of the specified purpose". At the present time, a majority of schools attempt to develop an objective and simple acceptance procedure and, therefore, e.g., all marks from the last two years of studies (or last six years of studies, as requested on applications for study at universities) are hardly usable. In fact, this only complicates completion of the relevant applications.

Acceptance to both secondary schools and universities can be based on approved criteria announced by the schools for acceptance procedures, which lie fully within the competence of the director of the school or dean of the relevant faculty. Thus, personal data that are required from the applicants should include only contact details, e.g. identification details, and, in addition, only information following from the relevant criteria: average marks in the last years of the previous school, the results of various competitions, e.g. modified working capacity or a subsidiary course acknowledged by the school. No other personal data are required and, on the contrary, could influence objective decision-making.

Universities have been introducing remote applications through the internet and, when creating internet applications, they understand that they require only certain personal data of the applicants.

The birth number is a separate issue. The birth number is a practical personal identifier and information that allows for unambiguous distinguishing of persons with the same name and the same date of birth, as the case may be. However, Article 13c of the amendment to Act No. 133/2000 Coll., on Register of Population and Birth Numbers, of 2004, strictly stipulates who may use birth numbers.

As schools do not conclude any agreements with the applicants (the applicant becomes a student of the school only after acceptance to study), only the name, surname, date of birth and place of residence are required to identify the applicants. No other law mentions the need to require birth numbers and, thus, there is no legal basis for any entitlement to collect the birth numbers of applicants for study.

Preserving documents from the acceptance procedure, especially with respect to unsuccessful applicants, is another fundamental issue. Article 5 (1) of the Personal Data Protection Act is unambiguous in this relation, stipulating that the "the controller shall be obliged to preserve personal data only for a period of time that is necessary for the purpose of their processing." It can be derived from the word-

ing of the Act that: as an applicant has not succeeded in the acceptance procedure, for which he provided his personal data, the purpose of their processing has ceased to exist and, therefore, there is no need to preserve his data. The practice to date, where these documents are kept by schools for a period of 10 years, appears to be at variance with the Act. The argument of the Ministry of Education that parents are entitled to appeal pursuant to the Code of Administrative Procedure, possibly even to the European Court, is irrelevant: the applicant or his statutory representatives may appeal against an administrative decision within a period of three years. Therefore, the documents related to appellants may be sent to the competent court only during this period; other documents from the acceptance procedure may be destroyed.

It is common in control of the personal data of applicants for employment that completion of a personal questionnaire is requested at a time when no employment contract is being concluded and, therefore, the requirement that certain questions contained in the questionnaire be answered is at variance with the Labor Code: where the Labor Code stipulates prohibition of discrimination for the reason of marriage and family status or family obligations, these personal data may not be required prior to execution of the employment contract.

However, it shows that it is often unnecessary to request this information even after execution of the employment contract: The controller (in this case, the employer) may collect personal data following from his statutory duties, e.g. calculation of the salary according to years of employment, completed education, experience in the given field; the number of children of a woman for the needs of pension insurance; calculation of taxes (deduction for minor children, or disability, spouse, partial pension), etc. It is not permissible to request the personal data (date of birth, employment, place of residence) of a spouse or adult children, in relation to whom deductions are applicable. Indeed, the employee is forced ("I declare that I have not concealed …") to provide the personal data of persons who are not aware of this fact. However, the controller (in this case, the employer) is authorized to collect the personal data of persons only with their consent. (Exemptions from this rule are described in Article 5 (2) of the Personal Data Protection Act; however, neither of these exceptions is applicable in the given case.).

Results of controls concerned with processing of personal data in the area of housing

Appropriate housing policy is one of the preconditions of existence and further development of the State. Active housing policies are pursued in the Czech Republic both by the State and by territorial self-governing bodies (cities and municipalities) and housing cooperatives. Appropriate instruments are used at all the above levels in order to achieve the set objectives in the area of housing and for practical implementation of the housing policy. Simultaneously, instruments are used by banks, i.e. individual loan products of financial institutions. A number of legal and natural persons offering various services are also active in the area of housing. The actual implementation of the housing policy at the level of cities and municipalities and the provision of services in the area of housing requires handling of personal data of those who are interested in acquiring a new apartment and particularly those who already have an apartment. Therefore, within its control activities, the Office also concentrated on control of performance of the duties stipulated by the Personal Data Protection Act for entities who implement housing policies at the level of cities and municipalities and also those natural and legal persons who operate a business in the area of housing by means of offering of services. These entities include particularly municipalities, housing cooperatives and legal and natural persons (commercial companies and operators of a trade) who were subject to control both in 2003 and in 2004.

Control activities of the Office were aimed particularly at the following areas of housing, with respect to handling of personal data of persons who are interested in acquiring a new apartment and particularly persons who already have an apartment:

A) Support for maintenance and recovery of the existing housing facilities

- recovery of the current concrete apartment buildings;
- recovery and modernization of old apartments in buildings of the existing urban structure;
- improvement of housing administration;
- occupation of apartments belonging to deceased persons;
- all measurements of energy and withdrawn cold and hot utility water in municipal apartments, and discharge of wastewater;
- transfer of signal of radio and television programs through cables to tenants;
- mandatory services;
- persons with outstanding payments of rent and enforcement of claims;
- black market in housing.

B) Support for all forms of housing construction

- support for new housing construction for target groups of the population

C) Development of housing market

- privatization of municipal apartments;
- control of use of municipal apartments and imposing sanctions on tenants breaching their obligations.

D) Support for housing for specific groups of the population ("social housing")

- securing housing for specific groups of the population in the framework of new housing construction;
- securing housing for specific groups of the population in the framework of the existing housing facilities.

E) Cooperation with the population and other entities

- potential of tenants to participate in resolving housing issues.

Summary of the results of a set of controls aimed at processing of personal data of those who are interested in acquiring an apartment (applicants for an apartment) and particularly those who already have an apartment (tenants, sub-tenants):

Five separate controls were carried out in accordance with the results of control activities of the Office from 2003 and 2004 and in response to instigations delivered to the Office in 2004; the controls were concerned with processing of personal data (of tenants, sub-tenants, owners of apartments and applicants for an apartment – natural persons) by five different controllers or processors who either owned or managed apartments and apartment buildings or offered services in the area of housing. The numbers of data subjects in certain controlled instances of processing of personal data were of the order of tens of thousands or even hundreds of thousands (e.g. in the Capital City of Prague).

Certain instances of processing of personal data are characterized by a substantial scope of transaction data related to the data subjects (tenants or sub-tenants) generated in the invoicing process, particularly for the provided services and consumed energy, consumed water or contractually set amount of discharged wastewater, or the transferred signal of television programs within the agreed scope (for common antennas).

During the above-mentioned five controls, it was ascertained with respect to some controlled entities (cities, city wards and city districts) that they require

contact and identification details of applicants without statutory authorization, and thus without justification, within submission of applications for an apartment for the purpose of facilitating the process of selecting the suitable applicant and, particularly, within assessing the decisive conditions set by the bodies of the city:

- copies are made of identity cards of the applicants for apartments and also of their spouses;
- copies are made of birth certificates;
- copies are made of marriage certificates;
- copies are mode of valid court decisions in case of divorce of the applicant and his/her former spouse;
- documents are required from the relevant doctor, documenting the state of health of the applicant.

The above-listed copies of documents are included by the controlled entities in files and kept for further potential use.

It follows from evaluation of the results of the five controls aimed at performance of duties of the controller and processor in processing of personal data of tenants, owners of apartments and co-owners of apartment buildings pursuant to the Personal Data Protection Act that:

- Several controlled entities breached the duty to collect only personal data corresponding to the set purpose and within the scope required for attaining the set purpose of processing pursuant to Article 5 (1) (d).
- Several controlled entities breached the duty to process personal data only with the consent of the data subject pursuant to Article 5 (2).
- One controlled entity failed, as a controller of personal data, to comply with the duty to conclude an agreement on processing of personal data with the processor pursuant to Article 6 of the Personal Data Protection Act.
- One controlled entity breached the duty to process personal data only with the express consent of the data subject pursuant to Article 9 (a) (This is a precondition required for processing of sensitive data).
- One controlled entity failed to perform the duty to provide due and timely written information to the data subject prior to commencement of processing of personal data within the scope pursuant to Article 11 (1).
- One controlled entity failed to perform the duty to provide due and timely written information to the data subject prior to commencement of processing of personal data within the scope pursuant to Article 11 (2).
- One controlled entity failed to perform the duty to provide due and timely written information to the data subject prior to commencement of processing of personal data within the scope pursuant to Article 11 (3).

Inadequate knowledge in the area of protection of personal data was ascertained with respect to employees of some controlled entities.

During the controls, it was ascertained that Article 13 of the Personal Data Protection Act creates a desirable pressure on territorial self-governing bodies (controllers) to adopt measures preventing unauthorized or accidental access to personal data.

Processing of personal data by a commercial company and detective agency

On the basis of an instigation and complaint in the media, a control of a commercial company and a detective agency was carried out in 2004. The instigation sent to the Office included a suspicion of unauthorized collection and processing of personal data of persons arrested by a detective agency on business premises

of a commercial company. Given the fact that the commercial company concluded a contract with the detective agency for the provision of detective services, the control was concerned with fulfillment of the duties stipulated by the Personal Data Protection Act in processing of personal data on the premises of the commercial company by that company, as the controller of personal data, and by the detective agency, as the processor.

The commercial company concluded a contract for the provision of detective services with the detective agency. The subject of the contract included the obligation of the detective agency to provide detective services to the commercial company, consisting particularly in prevention of misdemeanors and criminal offenses on the sales premises of the commercial company, including arresting of potential offenders.

Although the commercial company agreed on the provision of detective services on its premises with the detective agency within a scope that is apparently based on extensive interpretation of the legislation, the instigation in the media and the complaint submitted to the Office could not be neglected and control had to be carried out from the viewpoint of the Personal Data Protection Act. By evaluation of the contract and through control, it was ascertained that the commercial company was the controller of personal data of persons who were arrested by the employees of the detective agency on its sales premises during theft of goods and, therefore, the company was subject to the duties imposed on the controller of personal data by the Personal Data Protection Act. Pursuant to Article 4 (j) of the Personal Data Protection Act, any entity that determines the purpose and means of personal data processing is the controller, where the actual processing of personal data may be entrusted to the processor, within the scope of all operations in processing of personal data. However, even in case where all activities are transferred from the controller to the processor of personal data, the responsibility for the processing remains with the controller. The controller of personal data may not fully transfer his responsibility for the procedures in the processing to the processor, even on the basis of an agreement (in the given case, the detective agency processed personal data of arrested persons for the purpose of ascertaining their identity and submission of these persons to the Police of the Czech Republic or, in case of minors, to the statutory representatives, on the basis of a contract with the commercial company).

Thus, if the controller of personal data entrusts their processing to the processor of the personal data and this authorization or empowering does not follow from a legal regulation, pursuant to Article 6 of the Personal Data Protection Act, the controller must conclude with the processor an agreement on personal data processing. This agreement must have the requisites stipulated in that provision.

It was ascertained during the control that the contract concluded between the commercial company and the detective agency meets only the requirement for a written form and specification of the term, for which it was concluded. The duty imposed on the controller of personal data (the commercial company) in Article 6 of the Personal Data Protection Act is aimed at ensuring that the controller, if he entrusts the processing of personal data to some other entity (detective agency), provides for protection of the processed personal data, by specifying in writing the term, scope and purpose of the processing and requests from the processor guarantees related to technical and organizational securing of the protection of personal data.

The control demonstrated that the above-specified duty pursuant to Article 6 of the Personal Data Protection Act was breached by the commercial company. The lack or inadequate specification of the scope and purpose of processing of personal data in the contract concluded with the detective agency resulted in an unfavorable

state of affairs, where no precise procedures in collection of personal data and subsequent processing of these data had been stipulated, i.e. in a danger of processing of personal data at variance with the scope or manner stipulated by the Personal Data Protection Act. The absence of guarantees related to technical and organizational securing of protection of the processed personal data by the processor – the detective agency – substantially increased the risk of unauthorized processing, misuse or loss of the processed personal data. Therefore, on the basis of the above-described control finding at the commercial company, it was necessary to carry out control at the actual processor, i.e. the detective agency.

The detective agency, as the processor of personal data in the sense of Article 4 (k) of the Personal Data Protection Act, is obliged, pursuant to Article 5 (2), to process personal data only with the consent of the data subject. However, the control ascertained that the consent of the data subject was missing in all controlled cases. Furthermore, the control ascertained that the detective agency also processed sensitive data of the arrested persons. Pursuant to Article 9 (a) of the Personal Data Protection Act, sensitive data may be processed only if the data subject provides his express consent to the processing. The Personal Data Protection Act was also breached in relation to this duty. Furthermore, pursuant to Article 5 (1) (d) of the cited Act, the detective agency was obliged to collect only personal data corresponding to the set purpose and within the scope required for attaining the set purpose of processing. However, it was ascertained during the control that the detective agency also collected and subsequently processed personal data (in particular, the birth number and nationality), which was at variance with the set purpose and scope required for attaining the set purpose consisting in ascertaining the identity and submission of persons arrested on the sales premises of the commercial company to the Police of the Czech Republic.

Furthermore, when processing personal data pursuant to Article 11 (1) and (2) of the Personal Data Protection Act, the detective agency was obliged to inform the data subject (the arrested person) of the scope in which and the purpose for which the personal data would be processed, who and in what manner would process the personal data and to whom the personal data might be disclosed. On the basis of the control findings, it was necessary to state that this notification obligation was not fulfilled in any single case.

The detective agency, as the processor of personal data pursuant to Article 4 (k) of the Personal Data Protection Act processed personal data of persons suspected of theft on business premises of the commercial company without the consent of these persons and, furthermore, processed sensitive data of these persons without their express consent, collected personal data of persons that did not correspond to the set purpose and, moreover, failed to fulfill the notification obligation towards these persons.

As a consequence of the above-described instances of violation of the Personal Data Protection Act, measures had to be taken, including a duty to liquidate the personal data of arrested persons collected and processed without authorization and including a fine.

Internet services

Companies providing internet services (e-mail, web, chat, etc.) process records of persons who are registered as users of these services. The users provide personal data voluntarily and may elect which of these data will be disclosed to other users. Given the fact that this is a free service, which does not require any contract, it is upon discretion of the individual users, which data they will provide. The companies have no means of control of these data and, therefore, their accuracy, as required by Article 5 (1) (c) of the Personal Data Protection Act, is

extremely low. Thus, consequently, it is very difficult to characterize the above-mentioned databases as "containing personal data" according to their contents, but they can be unambiguously characterized as such according to their form.

Sharing customer databases

Several companies are sharing a common customer database within their commercial relations. They have mutually provided the file containing this unsecured database through the internet. The agreement concluded between the companies did not contain any provision concerning protection of the personal data, as required by Article 6 of the Personal Data Protection Act, i.e. "provision of adequate guarantees related to technical and organizational securing of the protection of personal data". The use of the internet for the transmission of messages containing personal data in an open form is generally unacceptable and does not meet the requirements stipulated in Article 13 of the Personal Data Protection Act. Therefore, measures were imposed, and accepted by the company, aimed at securing the transmission from technical and organizational viewpoints.

Sharing of databases of associated commercial companies

An unincorporated association of commercial companies acts under a common name and with a common marketing approach to customers. A fidelity program, whose entry form contained numerous personal data, was created for long-term customers. While the form also contained the consent to processing of these data, in the heading, it included the name of the association of companies; however, each member of the association processed these data separately. The form was modified in that the controllers of personal data were clearly defined and redundant data omitted (birth number).

Administration of the database of a professional association

Personal data of members of a professional association are processed by authorized employees and members of the association. In the framework of each district association, the number of these persons includes one authorized employee, who is obliged, under the employment contract, to maintain confidentiality, and members of the Board of Directors and the revision committee. Only authorized employees have access to the central records, while the individual files are accessible by all the above-mentioned persons to full extent. However, no records were kept of opening such files by the above persons. The authorized employees should have signed a confidentiality obligation on the basis of an amendment drawn up by the headquarters. According to the established practice stipulated in a decision of the self-governing body, each individual district association acts separately as an employer. Thus, the professional association is currently not competent to conclude the relevant amendments or control their performance, although the association is the sole legal entity in this context. In addition to remedy of this state of affairs, the Office also ordered that the authorized employees submit personal files of the members only with respect to cases under consideration and that they keep relevant records thereof.

Registration duty and matching of databases

A controlled entity processed personal data in that it matched personal data obtained from other persons that were originally obtained from a public list (land registry) with other published data and non-public data. Thus, it did not process exclusively personal data that had been previously published. The controlled entity, as the controller of personal data, failed to inform the data subjects, duly and in time prior to commencement of the processing, in what extent and for what purpose the personal data would be processed, who and in what manner would process the

personal data and to whom the personal data might be disclosed, or for whom they were intended. The entity failed to notify the Office of this processing and processed personal data of natural persons to an extent greater than required, as, simultaneously with personal data of persons, who were covered by the purpose of the processing, it also processed personal data of other persons, i.e. data whose processing did not attain the purpose of processing performed by the controlled entity. Thus, the controlled entity matched personal data that were obtained for various purposes without any legal basis stipulated in a special law. The measures imposed by the Office will ensure remedy of the defective state of affairs.

Records of owners

A breeder recorded personal data of persons to whom he had sold a pup. These data were related to accounting duties and regulations in the area of animal protection. Records of such owners of dogs may be kept by a special-interest association of breeders only with their consent. However, for the needs of the relevant association, it suffices to use records of dogs without identification of their owners and, therefore, these data are not personal data from the viewpoint of Personal Data Protection Act.

Personal data and accommodation services

An organization providing accommodation services used birth numbers as a variable symbol for payments for accommodation. Act No. 133/2000 Coll., on Register of Population and Birth Numbers, stipulates the rules for management of the birth number and use of the birth number. The birth number (hereinafter "BN") is defined as an identifier of a natural person within the information system of Register of Population and is unique for each natural person included in the information system. From the viewpoint of the Personal Data Protection Act, this is a special type of a personal data, whose processing is limited by a special law. However, for newly concluded contracts, it would be necessary to obtain the consent of the bearer of BN, without violating his will. However, the use of BN is not necessary for identification of payments for accommodation, as it can be replaced by a different identifier.

Personal data and documentation of public contracts

A company required, within the tender dossier for public contracts, that the contractors fill-out forms containing personal data of the "key construction personnel". The ordering party proceeded pursuant to valid Act No. 40/2004 Coll., on Public Procurement, which does not provide any further specification of the term "survey of technicians". However, from the sense of the Act and from the needs of the company it follows that a survey of the number of technicians and their expertise would suffice. Thus, the forms submitted in the framework of the tender dossier may contain only details indicating the education and professional qualification. Indeed, Article 5 (1) (d) of the Personal Data Protection Act stipulates that the controller is obliged to "… collect personal data corresponding exclusively to the specified purpose and in an extent that is necessary for fulfillment of the specified purpose". The measures imposed by the Office were aimed at fulfilling this provision.

COMPLAINTS HANDLING

From January 1 to November 31, 2004, when a change was made in processing of complaints in the framework of reorganization, the Control Department dealt with 335 petitions. These petitions were made through:

1) written or electronic petitions, mainly of citizens and legal persons;
2) petitions by governmental authorities;
3) on the basis of personal visits by complainants;
4) monitoring of the media.

The first task of the Control Department was to thoroughly review the complaints and establish the degree of their justification, by means of further enquiries aimed at obtaining objective information on the described state of affairs, either by monitoring of publicly accessible sources or by requesting further information or documents from the person submitting the complaint. Due to the potential for frustration of evidence, which could occur in these cases, in 2004, the Control Department, as a rule, no longer addressed the entity, against which the petition was aimed.

Where the circumstances indicated that a criminal offense had been committed, the matter was promptly submitted to the bodies active in criminal proceedings, where the Control Department further cooperated with these bodies. It continues to fully engage in resolving of these issues within its responsibility until the criminal proceedings are closed.

In the performance of control, the Office respected the principle that, as a rule, the identity of the complainant is not disclosed to third persons in the framework of the relevant enquiries; his identity is revealed, as a rule, only when necessary and with his consent. The Control Department also did not refuse to address anonymous complaints.

Unjustified complaints

It must be stated that a number of complaints were found to be unjustified after initial review, due to the following reasons:

In particular, the earlier experience was confirmed that a number of complaints are filed on the basis of the fact that the controller (usually a certain company, but also a state institution) has not fulfilled the expectation of the complainant concerning delivery of certain goods or provision of services, issue of a decision, etc. Thus, the subject of the complaint is not related to processing of personal data. Processing of personal data was only of secondary importance for the complainant; however, this changed when he was not satisfied in the proceedings held pursuant to some other regulations or when he came to the conclusion that this process (e.g. legal action) would lead to excessive burdens for him. In this relation, it should be recalled that submission of a complaint to the Office is not conditional upon payment of an administrative fee or demonstrating legal interest in the given matter.

In several cases, the complainants also requested that a decision be adopted with respect to satisfaction of their individual claims, e.g., declaring the obligation to pay a certain monetary amount, obligation to provide an apology, etc. It should be noted here that the Control Department dealt with such complaints from the viewpoint of potential adoption of measures falling within the competence of the Office. The complaints were also often concerned with ad hoc and non-systematic processing of personal data, e.g. in the form of a single piece of information published by the mass media. However, it is necessary to address this issue on the basis of other regulations, in particular, by bringing an action for the protection of personal rights pursuant to § 11 ff. of the Civil Code.

Repeatedly, the complaints were also concerned with processing of personal data that is regulated by a law that is a special law in relation to the Personal Data Protection Act and, therefore, such processing did not require the consent of the data subject. It should also be noted that there is a common incorrect opinion that personal data may be processed only with the consent of the data subject. This type of complaints was concerned primarily with keeping of the Commercial Register.

In some cases, the complainants lodged a complaint without previously exercising their right towards the controller in accordance with Article 5 (5) of the Personal Data Protection Act. In this case, the Control Department referred to the need to primarily exercise the given rights, where control would be commenced only in case of inadequate response by the controller. Similarly, several complaints were lodged without the complainant realizing that he had previously granted his consent to the relevant processing.

A great many complaints were formulated so vaguely or generally that effective control was not feasible. In a number of cases, the complainant refused to cooperate in any manner whatsoever with the Office after lodging the complaint, particularly to provide the necessary documents and other information for the purposes of further enquiries. Consequently, effective proceedings could not be pursued in those cases.

Justified complaints

First, it must be stated that a number of issues described in the Annual Report for 2003 continue to be relevant:

❶ A positive shift is clear in relation to direct marketing. However, some issues persist. In particular, it should be emphasized that, in 2004, the Control Department also dealt with some instigations related to unauthorized processing of personal data by an entity with a seat outside the territory of the Czech Republic. Although this feature is not directly related to the accession of the Czech Republic to the European Union, especially after the amendment to the Personal Data Protection Act, these issues become topical in the sense of cooperation of the European authorities in the area of protection of personal data.

In the Czech Republic, this specifically includes activities of the Polish company, Vegas sp. z z.o., with its seat in Warsaw, which undertakes regular letter campaigns, addressing Czech citizens. Czech households regularly receive letters sent by this company, containing a notice that the addressee of the letter has been selected by lot and could obtain a high financial award if he confirms this prize by telephone within the set deadline

❷ at a number specified in the attached leaflet. This is a number with an "increased rate", usually equal to CZK 60 per minute. The telephone call is then intentionally prolonged for at least 10 minutes and, for most of the time, it is pursued through an automatic answering machine. It need not be stated that the addressee of the letter receives no award whatsoever. This is an especially unscrupulous manner of eliciting money from trustful people. Particular emphasis should be placed on the psychological features of this fraudulent "business", where the addressee is reassured in his belief that he has finally got lucky and, therefore, should not let this opportunity escape. The wording of the leaflet is therefore conceived so that it emphasizes the passage of time: indeed, the addressee is incited to expedient conduct in order not to miss his opportunity.

Clearly, the primary question for the employees of the Control Department is where Vegas obtains personal data for addressing Czech citizens. Several enquiries were carried out in 2003 and especially in 2004, with respect to com-

panies in the Czech Republic that pursue similar activities (usually direct marketing) and where contacts with Vegas had been established in the past. It has been proven that databases containing personal data were transferred by these companies to Poland. These databases were concerned mainly with customers of "mail-order trade", which were very common in the Czech Republic especially the first half of the 1990s. Extensive data files were created in this relation, containing especially addresses and, in some cases, even the dates of birth (particularly in connection with undertakings comprising offers of various astrological studies and numerological analyses published in special journals).

However, given the scope of activities of the Vegas company in the Czech Republic to date, it showed that these databases themselves cannot provide the necessary source of data for all campaigns of the company. A substantial part of sources used by Vegas remains unknown. The situation is complicated by the fact that the style of business activities of similar companies does not require any complex technical and personnel background. Consequently, the seat of the company in Warsaw is basically formal and includes only a leased office in a building, where dozens of companies have their seat. The actual administrative activities related to the performance of campaigns and sending letters are pursued by companies, with which Vegas concludes contracts on processing of data. Given the above facts, even the Polish Office for Personal Data Protection has not been able to carry out control in the company. Similar to the Czech Republic, controls have been carried out to date only in companies that ensured processing of personal data for Vegas. However, these controls yielded a certain finding: the database of personal data used by Vegas need not necessarily be located in Poland. There is an assumption that Vegas uses an authorized access to a remote database located on a foreign server. This only illustrates the complexity of controls of such entities. Nevertheless, or consequently, employees of the Control Department were in regular contact with their peers from the Polish Office for Personal Data Protection. A joint control exercise was commenced at the end of last year, when inspectors of the Office were invited to a meeting in Warsaw. In 2004, the inspectors of the Polish Office performed control in companies that processed data for Vegas. Similar controls are expected to take place in the future.

❸ A number of complaints refer to excessive utilization of birth numbers on the basis of an incorrect opinion that a birth number is an absolute identifier of a natural person and thus a natural supplement to the name and surname. However, a fundamental change in this area was brought by adoption of amendment to Act No. 133/2000 Coll., on Register of Population and Birth Numbers, through Act No. 53/2004 Coll., which came into effect on April 1, 2004. It can be stated that the number of complaints has been constant after cessation of the first wave following after adoption of the above law. However, the received complaints showed certain gaps in the special legal regulation concerning the use of birth numbers and the transition period will need to be devoted to adoption of the necessary legislative measures.

❹ The Office continues to proceed against activities consisting in copying personal documents, which is often required as a precondition for the provision of services. The Office consistently bases its considerations on the standpoint that personal documents (e.g. the personal identity card) contain substantially more information than required for conclusion of a contract and thus keeping the relevant copies is not necessary. The frequent reference to the need for ensuring accuracy of personal data is irrelevant. This state of affairs should be improved by amendment to Act No. 559/2004 Coll., on Identity Cards.

❺ The Office for Personal Data Protection adopted measures against publishing documents on activities of municipalities containing personal data through the

internet. The above opinion is based on the fact that laws regulating competence of municipalities stipulate a regime of limited access to these documents, particularly for the needs of citizens of the given municipalities, cities, etc. However, the Personal Data Protection Act permits publishing of these documents after the relevant personal data are appropriately rendered anonymous.

The Office promotes similar principles also in relation to publishing certain documents of housing cooperatives on official boards located on public premises.

New issues in the area of protection of personal data ascertained in 2004

Several instigations were lodged during the last year, indicating a discovery of documents containing personal data. This documents that the approach of the controllers to fulfillment of Article 13 of the Personal Data Protection Act was not entirely accountable.

The issue of processing personal data concerning spectators of sports events, particularly football matches, is relatively new. However, in this respect, it has shown that the current legal regulations, particularly Act No. 115/2001 Coll., on Promotion of Sports, reflects inadequately the potential for cooperation between sports clubs and the police, aimed against unsuitable behavior of spectators, which is contemplated by the European Convention on Spectator Violence and Misbehaviour at Sports Events and in Particular at Football Matches, of 1985, which was ratified by the Czech Republic in 1995.

Similarly, a new topic consists in submission of personal data concerning owners of pedigree dogs. *(cf. p. 25)*

The Control Department also dealt with the issue of unsolicited commercial communications *(cf. p. 42)*: Upon adoption of Act No. 480/2004 Coll., on Certain Information Society Services and on the Amendment to Certain Other Acts, it began to fulfill its role of a supervisory body for the area of sending commercial communications by electronic means. For the purposes of this Act, a commercial communication includes all forms of communication intended for direct or indirect promotion of goods or services or image of an enterprise of a natural or legal person, which performs a regulated activity or is an entrepreneur pursuing activities that are not regulated; pursuant to the special regulation, commercial communications include advertising. Commercial communications do not include data enabling direct access to information on activities of a natural or legal person or an enterprise, particularly the domain or e-mail address; furthermore, commercial communications do not include data concerning goods, services or image of a natural or legal person or an enterprise, obtained independently by the user.

Pursuant to this Act, electronic means include particularly the network for electronic communications, electronic communication equipment, end telecommunication equipment and electronic mail. Thus, commercial communications can be sent, not only by electronic mail, but also by fax or by means of an SMS message, and also include "telemarketing", i.e. services offered by telephone.

The task of the Office for Personal Data Protection is to ensure that commercial communications sent by electronic means meet the set requirements and ensure, in particular, that the opt-in principle is strictly complied with, i.e. that commercial communications are sent only to entities that express their prior consent thereto. An entity sending a commercial communication must be able to demonstrate this consent at any time.

Act No. 480/2004 Coll., on Certain Information Society Services and on the Amendment to Certain Other Acts, came into effect on September 7, 2004 and does not provide for any transition periods. Therefore, measures aimed at harmonizing the current procedures with the new legal regulations should be imple-

mented without delay. Similarly, immediately after September 7, 2004, the Office should impose fines on entities sending unsolicited commercial communications after this date. From the date of effect of the Act, the Office has recorded a great many complaints related to its violation. *(cf. the table on p. 8)* Although, as mentioned above, the Act does not provide for any transition periods, the Office resolved not to impose fines for violation of the Act until the end of 2004 and concentrated on consistent remedial measures by entities, where violation of the Act was ascertained.

ADMINISTRATIVE PUNISHMENT

I. General part

In 2004, the Office used administrative punishment as a standard instrument in the framework of its supervisory activities, i.e. imposing fines for breach of the duties stipulated by the Personal Data Protection Act, usually related to shortcomings ascertained during control. No penalties have been imposed from the date of effect of the Personal Data Protection Act on the basis of a statutory exemption, as the controllers and processors of personal data had the benefit of a transition period for bringing their processing of personal data into accord with the requirements of the new Act.

Financial penalty for proven misconduct usually accompanies remedial and indemnification measures and thus it facilitates remediation of the defective state of affairs in the course of the Office's supervisory activities. The Personal Data Protection Act still distinguishes between misconduct of controllers and processors, who are liable to a fine of up to CZK 10 million (CZK 20 million for repeated torts), and misdemeanors of natural persons, which are subject to a fine of up to CZK 25,000, or, as the case may be, CZK 50,000. Simultaneously, the Act does not stipulate the amounts of fine applicable for individual torts; however, account must always be taken of the general criteria stipulated by the Act, including the nature, seriousness and manner of conduct, degree of fault, duration and consequences of the misconduct.

With effect as of January 1, 2005, the amendment to the Personal Data Protection Act brought by Act No. 439/2004 Coll. provides for more detailed differentiation between the merits of individual torts and, simultaneously, further specifies the conditions for imposing penalties, in accordance with the principles of administrative punishment prepared by the Ministry of Interior. The highest amount of a fine will be applicable to illegal procedure in processing of personal data and in case of endangering individuals caused by intervention in their private and personal lives and will equal CZK 10 million. Both the amounts of penalties and the merits of the individual delicts are differentiated with respect to the conduct of certain natural persons (misdemeanors) and of legal persons and natural persons operating a business (other administrative delicts). It is also expressly stipulated with respect to legal persons that they are not liable for an administrative delicts if they used all reasonable efforts to prevent the breach of the legal duty. Specification of the need to commence the discussion of an administrative tort within 1 year from establishing the delict and to close the discussion of the delict at the latest within 3 years of its committing is important, not only from the viewpoint of entities obliged to comply with the Act, but also from the viewpoint of comprehensive and extensive controls carried out by the Office.

Amendment of the above-mentioned part of the Act ensures, inter alia, better enforceability of the protection of public interests; however, simultaneously, it affects the possibility to claim satisfaction or even obtaining indemnification if such private claim is raised by the injured person. Private claims following from violation of the Personal Data Protection Act will undoubtedly be more frequent also in less serious cases, mostly mistakes at work, i.e. misconduct other than breach of confidentiality committed by natural persons who are neither controllers nor processors (usually employees). The Office is no longer competent to discuss such misconduct – and the related private claims.

Pursuant to the Act, the Office is obliged to deal with each suspicion concerning violation of the Act. Administrative proceedings on imposing a sanction are a process with strictly defined authorization of the administrative body, serving for proper and full investigation of cases of misconduct and, simultaneously, defending the rights of the parties to the proceedings, i.e. the suspects. The above-described proceedings, which can be commenced on the basis of a justified suspicion and on the basis of at least partly specific allegations (often only in connection with findings obtained during control), is not intended to satisfy claims of the petitioners, who are often the injured persons. However, in that case, the Office, which repeatedly encounters such expectations, may only provide consultations and advice on legal service; however, it thus partly replaces the inadequately developed social segment of special-interest and civic associations that would assist in dealing with various situations, where the competence is not entrusted to the State.

The following table gives the number of suspicions of violation of the Act that were discussed by the Office within administrative proceedings and proceedings on misdemeanors in 2004. Description of the most serious cases, where the Office imposed a fine, is enclosed.

II. Number of instigations and proceedings held

Number of instigations related to suspicion of administrative delicts	
Total	45
of which – based on own findings	19
– on the basis of referral by the bodies active in criminal proceedings and bodies dealing with misdemeanors	5
– on the basis of instigations from natural and legal persons	21
Handled*	53
– through discontinuation prior to commencement of proceedings	8
– through a decision on imposing a fine (total)	35
– of which with legal force	32
– discontinuation of proceedings	9
– referral to some other body	1

**Including handling of instigations, whose discussion was commenced in 2003.*

III. Special Part

The highest validly imposed fine for an administrative tort pursuant to Article 46 (1) of the Personal Data Protection Act, equal to CZK 500,000, was imposed in 2004 on a employment agency, which, as a controller of personal data of applicants for employment, breached the duties stipulated in Articles 9, 10 and 13 of the Act in that it processed sensitive personal data of applicants for employment without having their express consent to such processing in the sense of Article 9 (a) of the Personal Data Protection Act and, furthermore, failed to ensure in pro-

cessing of these personal data that the data subjects (applicants for employment) do not incur any harm to their rights, particularly the right to preserving human dignity. The agency also failed to adopt any measures preventing unauthorized or accidental access to personal data, their change, liquidation or loss, unauthorized transfers and other unauthorized processing, as well as other misuse of personal data.

The administrative proceedings against this company were commenced on the basis of discovery of written documents containing personal data of applicants for employment near municipal waste bins. These written documents contained numerous personal data of applicants, including sensitive data on their state of health, lack of criminal record and nationality, and also written assessment of the applicants by consultants and employees of the employment agency, containing various subjective, abusive or even gross remarks on the applicants.

An administrative decision on this matter was issued on September 18, 2003; however, the case was finally closed on November 4, 2004, when the Municipal Court in Prague rejected a petition against the administrative decisions (of both the first and second instances) of the Office.

Another controller of personal data, who substantially breached the duties stipulated by the Personal Data Protection Act, was a bank, which, as a controller of personal data, in the framework of a campaign aimed at obtaining new clients, collected and subsequently processed personal data of the potential clients, without fulfilling, with respect to these persons, the notification obligation of a controller, following from Article 11 (1) to (3) of the Personal Data Protection Act. Furthermore, with respect to some personal data, it was not able to demonstrate the consent of the data subject to the processing of personal data.

It followed from the control findings of the Office, that the employees of the bank were requested to collect personal data of their friends or business partners. They were motivated to such conduct by non-financial remuneration, provided that inadequate activity of certain employees in this area resulted in a request for fulfillment of the set tasks, which amount, in some cases, to a threat.

The minimum scope of data collected with regard to the individual data subjects included surname and telephone number; however, the contact details of other persons comprised personal data including all items requested by the bank, i.e. particularly the name, surname, place of residence, estimated age, telephone number, and, in certain cases, also other "non-compulsory" items, such as the title, business name, number of children, profession, other contacts, recommended manner of approach, and also data on the bank of the given person, whether he has concluded a mortgage, etc.

A decision was issued on the basis of the above findings on June 25, 2004, whereby a fine of CZK 485,000 was imposed on the bank for breach of the duties stipulated in Article 5 (2) and (5), and Article 11 (1), (2) and (3) of the Personal Data Protection Act, i.e. an administrative tort pursuant to Article 46 (1) of the cited Act.

A fine of CZK 230,000 was imposed through an administrative decision of August 27, 2004 on a company operating a chain of hypermarkets in the Czech Republic for breach of the duties stipulated in Article 5 (2) and Article 13 (1) of the Personal Data Protection Act.

In this case, the administrative proceedings were again commenced on the basis of control findings of the Office for Personal Data Protection, from which it followed that the relevant company collected and preserved personal data of persons suspected of theft, without their consent, in connection with thefts occurred on one of its business premises. It also failed to adopt the necessary measures against unauthorized and accidental access to these personal data. Consequent-

ly, the former employee of the company was able to offer a list containing personal data of the alleged thieves for publication in periodicals.

A company operating a chain of markets is undoubtedly authorized, in order to protect its rights and legally protected interests, to collect data that are required for subsequent communication with the Police of the Czech Republic (or with the municipal police) in cases of theft of goods, where these data undoubtedly include information concerning the stolen goods and the number of the protocol that allows for association of the data on the goods with the details of the expected offender, kept by the police. In the given case, the identification personal data of arrested persons may be collected explicitly for the purpose of their submission to the police and only if the relevant persons provide these data voluntarily. However, processing of personal data of persons suspected of theft in one's own database cannot be considered to be processing required for the protection of the rights of the controller; moreover, given its nature, i.e. on the basis of an allegation that the data subject was arrested during theft, this information is clearly capable of infringing on his right to protection of private and personal life.

Thus, by his conduct, the controller of personal data committed an administrative tort pursuant to Article 46 (1) of the Personal Data Protection Act, for which he was punished with the above-mentioned fine.

Administrative proceedings were also held against armed corps of the Czech Republic on the basis of control findings of the Office.

A decision on a fine was issued in the relevant proceedings on August 20, 2004, stating that, in the framework of his information system, the controller of personal data processed inaccurate personal data without designating these data as inaccurate. Furthermore, he also processed personal data of his employees and employees of the relevant ministry, whose processing in the relevant manner did not correspond to the purpose set for the given information system, and also failed to specify the period of preservation of personal data required for attaining the set purpose of their processing. Consequently, he preserved personal data in the information system for an unlimited period of time and, thus, clearly for a period longer than required for the purpose of their processing. He also failed to adopt any measures preventing unauthorized processing or other misuse of personal data and failed to bring the processing of personal data performed prior to the date of effect of the Personal Data Protection Act into accord with this Act.

Through the above-described conduct, the controller of personal data breached the duties stipulated in Article 5 (1) (c), (d) and (e), Article 13 (1) and Article 47 (2) of the Personal Data Protection Act and, thus, committed an administrative tort pursuant to Article 46 (1) of the Personal Data Protection Act, for which he was punished with a fine of CZK 130,000.

REGISTRATION PROCEDURE

The main acts in the framework of the registration procedure include:

- acceptance of notifications of processing of personal data;
- applications for permitting transfer of personal data to other countries;
- review of notifications and requests in the framework of proceedings;
- keeping records.

The course of the registration process was substantially affected by the amendment to the Personal Data Protection Act with effect as of July 26, 2004. It introduced important changes that were reflected in the manners of handling notifica-

tions. Pursuant to Article 16 (6), handling of registration notifications is not longer governed by the Code of Administrative Procedure, whereby the registration proceedings are simplified from both administrative and procedural viewpoints. The Office is able to remedy defects of notifications in a more flexible manner, without burdening the notifying party. However, it further holds that in cases, where sufficient information is not provided to carry out the registration, the notifying party is invited to supplement the information and the relevant party is then obliged to supplement the requested information within the set deadline. Otherwise, the notification is regarded as not submitted.

The controller is authorized to commence processing of personal data after expiry of the statutory term, i.e. after 30 days from the date when the notification of the processing was delivered to the Office, unless the controller has been invited to supplement the notification and unless administrative proceedings have been initiated on reviewing the legality of the notified processing of personal data pursuant to Article 17 of the Act.

If interested, the controller may request that the office issue a certificate of registration pursuant to Article 16 (5). The issued certificate demonstrates the registration of processing of personal data and its recording in the register kept by the Office.

From the date of effect of the amendment, the list of registered controllers is no longer published in the Journal of the Office. Only a list of cancelled registrations is published. Information on the individual instances of processing of personal data recorded in the register, except for information set forth in Article 16 (2) (e) and (i), is publicly accessible in electronic form on the website of the Office (www.uoou.cz/registr.php3).

In connection with adoption of the amendment, it was also necessary – in cooperation with the department of informatics of the Office – to carry out a change in the database system of the register, which will be interconnected with the newly established electronic filing service in 2005. This will ensure greater effectiveness in electronic processing of the stored data, more efficient management of the records of notified instances of processing and their more effective use for the needs of control activities of the Office.

From the viewpoint of assessing the individual notifications, processing that is yet to be commenced is examined and reviewed in more detail: primarily, the purpose of processing is examined, with a view of distinguishing the controller from the processor; appropriateness of the scope of personal data to the set purpose of processing is considered; the nature of processing is reviewed with respect to the exemptions from the notification obligation pursuant to Article 18 of the Personal Data Protection Act; and completeness of the reported information is also assessed. Special attention is given to processing of sensitive data.

Further specification of the registration process led to reduction of the total number of notifications; however, the number of requests based on incomplete or unclear information increased. Thus, the amount of administrative activities actually increased. In a number of cases, the purpose of processing, the scope of processed personal data and other information required for assessing the specific processing is clarified only on the basis of analysis and evaluation of responses of the notifying parties to a request for supplementation. Such registration proceedings are often concluded with a statement that the given notification is not subject to the notification obligation, either due to an exemption from the notification obligation pursuant to Article 18 of the Personal Data Protection Act or due to the fact that the notification is made by the processor, rather than the controller, of the personal data. If the notification is not subject to the registration obligation, the notifying party is informed of this fact.

The fast development of information technology, new areas of competence of the Office in the field of supervisory activities and the increasingly frequent cases of processing of a wide scope of personal data, including e.g. biometric data, have resulted in the need for a change in the employed registration forms, which no longer suit the current needs. First steps have been taken in this relation to modify the scope of data required for fulfillment of the notification obligation. This modification comprises, in particular, more detailed statement of the purpose and scope of the processed personal data.

Introduction of new registration forms should lead to an increase in the demands on analysis and evaluation of a higher number of accepted information and, thus, to higher demands on qualification and competence of the employees. Creation of new forms is a basic precondition for ensuring greater effectiveness of activities of the Office in the area of registration. However, the responsibility of the employees of the Office entrusted with registration tasks was also increased in the framework of reorganization of the Office and, with effect as of December 1, 2004, the Registration Unit was separated from the former Department of Administrative Decision-Making and was entrusted with full competence with respect to assessing individual notifications of processing of personal data and permitting transfer of personal data to other countries. An important part of the activities of the employees who provide for the registration process – from December 1, 2004, the Registration Department – again, during the relevant year, comprised information and consultancy activities. A number of enquiries continued to be concerned with the scope of duties of the controller of personal data following from the Personal Data Protection Act and with the manner of notifying processing, and certain enquiries were accompanied by a request for assistance in filling-out the registration forms. However, it can be stated that the number of these enquiries is constantly decreasing, which undoubtedly documents the greater knowledge and awareness of the duties of controllers with respect to the notification obligation. A majority of enquiries were related to application of Articles 16 and 27 of the Personal Data Protection Act. However, an opinion is still prevailing that each processing must be notified to the Office and no account is taken of the exemptions from the notification obligation pursuant to Article 18 of the Personal Data Protection Act, which were further specified by the amendment. A very frequent feature consists in notification of processing that is subject to the exemption from the notification obligation pursuant to Article 18 (1) (b), i.e. such instances of processing that are imposed on the controller by special laws or instances where such personal data are required to enforce the rights and duties following from special laws. These exemptions cover, e.g., facilities providing social care, educational facilities, housing cooperatives, etc. that process personal data only in the framework of activities imposed by special laws. The Office frequently receives notification from the public authorities (municipal or regional authorities, governmental authorities), which notify the Office of instances of processing that is performed on the basis of authorization to perform public administration and are also contemplated by the law. Another group of such notifications includes processing that is often notified to the Office for the purpose of registration and that is again not subject to the notification obligation given the exemption pursuant to Article 18 (1) (b) of the Act. These cases involve processing of employees' data in the framework of personnel and salary issues. Thus, the notification obligation does not apply particularly to entities performing activities that are expressly imposed by laws and entities that need to exercise the relevant rights and duties in the framework of legal regulations.

Submission of notification by persons, who process personal data for the controller of the personal data on the basis of a contract – typically, business agents

or insurance agents – is a relatively frequent mistake. In Article 16 (1), the amendment to the Act expressly imposes the notification obligation exclusively on controllers of personal data. Notification may be submitted only by the controller, who is the only person with comprehensive knowledge of the prepared processing of personal data. Therefore, the notification obligation does not apply to processors. However, there are frequent cases where the controller unlawfully requests that "his" individual processors submit a certificate of registration of their own processing, for which the controller is accountable; the Act imposes the duty to submit a notification of processing of personal data to the Office exclusively on the controller of personal data. If follows from the above that this area requires further awareness raising that could ultimately ensure, not only better awareness among the controllers and processors with respect to the notification obligation, but also less work for the Registration Department of the Office in dealing with the subject of registration notifications.

Activities of the Registration Department also include issuance of decisions on authorizing the transfer of personal data to other countries pursuant to Article 27 of the Personal Data Protection Act. The objective of this provision is to ensure protection of personal data of the data subject that are to be transferred and subsequently processed in other countries. The main viewpoint in decision-making in this respect consists in the adequacy of legislative protection of personal data in the country to which the data are to be provided. Also in this area, the amendment to the Personal Data Protection Act brought substantial changes.

Primarily, free flow of personal data that are to be transferred to a Member State of the European Union may no longer be limited pursuant to Article 27 (1). It appears that the controllers have no great difficulty with interpreting this provision: applications of this type were rare. Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, ETS 108, 1981), whose Article 12 limited the duty of the controller of data to apply to the Office for authorization pursuant to Article 27 (4) of the Personal Data Protection Act, was implemented already in 2003. However, enquiries concerning interpretation of this provision are still relatively frequent.

Personal data may be submitted to "third countries" (i.e. outside EU) if the prohibition of restricting free flow of personal data follows from an international treaty, whose ratification has been approved by the Parliament of the Czech Republic and is binding on this country, or if the personal data are being transferred on the basis of a decision of an institution of the European Union. The former case concerns particularly countries that have ratified Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and whose legal regulations thus ensure adequate protection of personal data. The latter case currently involves decisions of the European Commission, whose Czech wording is published in the Journal of the Office. In this relation, frequent enquiries are concerned with the duties of the controllers in submission of personal data to third countries on the basis of a Commission decision that are related to standard contractual clauses or in the framework of the "Safe Harbour" (treaty between EU and the U.S.).

Both the above-mentioned means of transfer of personal data are not subject to official authorization pursuant to the Act. However, in certain cases, under the conditions of Articles 16 and 18 of the Act, the intended processing of personal data, which will take place after the transfer, must be notified to the Office through the procedure pursuant to Article 16 of the Act.

Transfer of personal data to third countries, where appropriate protection of personal data is not ensured, may be permitted only upon fulfillment of one of the conditions stipulated in Article 27 (3) of the Act. Simultaneously, the Registration

Department has the duty, pursuant to Article 27 (4) of the Act, to verify in the framework of the proceedings on authorization of transfer of personal data, in particular, the source, final destination and category of personal data, and the purpose and period of their processing.

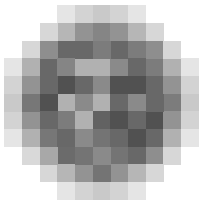
Registration statistics

	Total figures as of December 31, 2004	2004	2003	2002
Total number of notifications	26 042	1 972	3 187	3 801
Cases of processing registered	24 588	1 591	2 854	4 301
Controllers registered	21 709	1 402	2 604	3 967
Proceedings suspended*	7 871	785	1 094	1 010
Proceedings discontinued	229	91	46	92
Registrations cancelled	624	64	52	112
Processing not authorized	332	46	86	203
Number of notifications on a change in the processing	448	192	216	40

** From July 26, 2004 – requests pursuant to Article 16 (4) of the Personal Data Protection Act.*

Statistics of applications for transfer of personal data abroad pursuant to Article 27 in 2004

Total number of applications	52
Of which:	
Decisions on authorization of the transfer of personal data abroad	35
Proceedings suspended	17
Of the number of proceedings suspended, ultimately:	
Decisions on authorization of the transfer of personal data abroad	12
Decisions on rejection of the transfer of personal data abroad	0
Proceedings discontinued pursuant to Article 30 of Act No. 71/1967 Coll. on request of the party to the proceedings	3
Administrative proceedings not completed to date	2



Activities of the Office in the Legislative and Legal Area

I. POSITION AND COMPETENCE OF THE OFFICE

The position and competence of the Office, as an independent supervisory body of the state, is defined by Act No. 101/2000 Coll., on Personal Data Protection and on Amendment to Some Laws, as Amended. In 2004, the Personal Data Protection Act was affected by two direct amendments and it is therefore currently valid as amended by laws adopted during the previous years, i.e. as amended by Acts No. 227/2000 Coll., No. 177/2001 Coll., No. 450/2001 Coll., No. 107/2002 Coll., No. 309/2002 Coll., No. 310/2002 Coll. and No. 517/2002 Coll. and newly also by Act No. 439/2004 Coll. and Act No. 480/2004 Coll.

In 2004, the Office was entrusted with further areas of competence, pursuant to the amendment to Act No. 133/2000 Coll., on Register of Population and Birth Numbers (Act No. 53/2004 Coll., amending some laws related to the area of population registers), in matters involving unauthorized management of the birth numbers or unauthorized use of the birth numbers. On the basis of Act No. 480/2004 Coll., on Certain Information Society Services and on the Amendment to Certain Other Acts, the Office was entrusted, within the defined scope, with imposing penalties in the area of unsolicited commercial communications.

II. ACTIVITIES IN THE LEGISLATIVE AREA

At the beginning of the year, the Parliament of the Czech Republic completed the legislative process of amending the Personal Data Protection Act. The relevant amendment, which can also be designated as a "European amendment", ensured full harmonization of the Personal Data Protection Act with the basic European directives. The amendment to the Act was prepared in the context of the upcoming membership of the Czech Republic in the European Union and the ensuing need to harmonize the general conditions for protection of privacy in connection with personal data processing, as stipulated in the legislation of the Czech Republic, with the conditions following from international commitments of the Czech Republic in this area that are specified, in particular, in Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (hereinafter "Directive 95/46/EC"), and in Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "Convention No. 108"), which was ratified by the Czech Republic in 2001 (see Communication of the Ministry of Foreign Affairs published in the Collection of International Treaties under number 115/2001). Although the expected date of effect of the amendment, corresponding to the date of accession of the Czech Republic to EU, could not be met given the complexity of the legislative process, the adopted amendment (Act No. 439/2004 Coll. came into effect on July 26, 2004) entered into effect before the Personal Data Protection Act could become an object of criticism from the EU institutions.

The amendment fundamentally affected the scope of exemptions in cases, where derogation is possible from the basic principles of processing of personal data. At the present time, exemptions are possible only in important interests of the State (Article 3 (6)), on the basis of a special law. Certain definitions were also modified and supplemented to a certain degree.

In this connection, it should be noted that the basic terms of the Act, such as "processing" and "personal data" were little affected by the amendment. The term processing (Article 4 (e)), which, from the very beginning, has required a systemic approach to any operation with personal data, remained unchanged by the amendment. While the amendment to the Personal Data Protection Act affected the latter basic term – "personal data" – and the term "sensitive data", this modification was only partial. The part of the definition of the term "personal data" (Article 4 (a)), containing negative delimitation of this term, was omitted. Given the dynamic development of information technology, the former wording of the relevant sentence had become slightly obsolete and misleading. On the contrary, new criteria were supplemented to the definition of the term "personal data" concerning identification and identifiability of the data subject (physical, physiological, psychical, economic, cultural or social identity) and, similarly, these criteria were also supplemented in relation to the type of information (number, code, factor). Thus, information of a various character in a wide sense continues to be potentially personal data. With respect to sensitive data, the original character of this provision (Article 4 (b)), which contained, also prior to the amendment, an exhaustive enumeration, remained unchanged; however, it was supplemented by new important categories of sensitive data, such as "genetic data" and "biometric data". These, currently already well-known, categories of information are increasingly becoming the center of interest due to their unique nature and unambiguousness in relation to an individual – natural person. Therefore, it is correct that certain basic rules for their processing have been created in the legislation of the Czech Republic.

The most important change in the definitions stipulated by the Act comprises incorporation of a newly formulated basic definition of the consent of the data subject to processing (Article 4 (n)). For the first time, it has been explicitly stated that the consent is a legal act. Even if the Act included no other provisions related to the consent, these four words would perfectly express the basic intention of the legislator, namely to approximate, through this expression, the definition to the basic regulation of legal acts under civil law in the sense of Article 34 et seq. of the Civil Code. The consent is thus construed as a basic manifestation of the will of a natural person, the data subject, aimed at establishment of the right of the controller (processor) to process personal data. The consent, as a manifestation of will, may be provided, not only explicitly, as the Personal Data Protection Act contemplates in relation to processing of sensitive data, but also in some other manner, which casts no doubt as to what the data subject intended to express – in this case, he intended to express his agreement to processing of his personal data (Article 4 (n)). A substantial feature of the regulation of legal acts under civil law consists in freedom, seriousness, certainty and comprehensibility of the manifestation of will, provided that non-fulfillment of this precondition renders the act void. Thus, the same approach needs to be taken to the process of requesting consent, where the controller (processor) must convince the data subject of the intention to process his personal data and inform him of all essential facts (Article 11 (1) before the processing takes place.

The possibilities of processing sensitive data were stipulated more specifically in a manner usual in EU and contemplated in Directive 95/46/EC. The right of the data subject to obtain information on data processed thereon was strengthened, and strengthened and further specified was also the right to claim remedy of a defective state of affairs. The controllers and processors are newly obliged to docu-

ment the adopted security measures in processing of personal data. The new regulation of penalties is also important. While the basic differentiation to misdemeanors and other administrative delicts was maintained, both types of misconduct are now specified more accurately and are classified to individual merits and, according to the seriousness of violation, they are assigned various penalties. In other words, since the beginning of 2005, administrative penalties may be imposed only for violation of the individual provisions of the Personal Data Protection Act that are subject to penalties according to the terms of the Act.

As a consequence of the amendment, the Office for Personal Data Protection was also forced to meet other legislative requirements following from the amendment. This included primarily the task to draw up full wording of the Act. Due to nine amendments adopted during the last four years, the Act had become unclear for its addressees, although the Office maintained the valid full wording on its website. This legislative technical task was completed relatively quickly and the full wording was thus published in the Collection of Laws under number 525/2004 Coll. at the beginning of October 2004.

A Government regulation was also prepared in accordance with the wording of the amendment to the Personal Data Protection Act, concerning the form of the service card of inspectors and other control workers of the Office, who will be obliged to prove their identity through these cards within controls carried out by them. The duty to prepare and issue this regulation follows from the authorization in Article 38 (5) of the Personal Data Protection Act. At the time of preparation of this Annual Report, the draft regulation had already been discussed by legislative bodies of the Government without any serious problems and, therefore, it can be expected that the Government regulation will be published in the Collection of Laws in 2005.

The Office also participated in the creation of legal regulations prepared by other institutions: during 2004, the Office provided comments on more than 70 laws, 140 subordinate regulations and over 50 other legislative drafts. This is a clear increase compared to 2003, which follows from the fact that other proponents of legal rules have learnt to respect the fact that the Office has become an obligatory commentary place in cases where the legal regulation is related in some way to processing of personal data. A trend from 2003 can be confirmed: the principles of protection of personal data continue to be successfully incorporated in legislative drafts. The comments of the Office are usually fully accepted and, thus, the prepared legal regulations or their amendments, as appropriate, are brought into accord with the Personal Data Protection Act. The legislation thus begins to duly reflect the basic principles of the right to protection of privacy in cases where personal data of citizens are being processed – both in the commercial sector and in the entire public administration.

Involvement of the Office in the preparation of the new Act on Electronic Communications, which has been submitted by the Ministry of Informatics and is currently being discussed by the Chamber of Deputies, should also be mentioned. This governmental draft transposes to the Czech legislation EU directives, including Directive 2002/58/EC of the European Parliament and of the Council concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on privacy and electronic communications). This new regulation should contain specific details of the protection of personal data in the area of electronic communication and should impose on entrepreneurs in the relevant area the duty to ensure security of the provided services, including confidentiality of communication and some other duties aimed at protection of privacy of users and participants.

III. ACTIVITIES IN THE AREA OF GENERAL APPLICATION OF LAW

The interest of the general public, as well as of individual controllers and processors of personal data, in provision of positions, consultations and discussions concerning application of the Personal Data Protection Act in the framework of the legal order of the Czech Republic continued in 2004. In the framework of these activities, the Office provided over 3000 legal telephone consultations, which is an increase by more than 30% compared to 2003, and handled over 1200 written (and e-mail) petitions, corresponding to an increase by more than 20 % compared to the previous year.

The fact that the Office was entrusted with new areas of competence following from special laws had a considerable effect on the application and consultation activities of the Office for Personal Data Protection. The major amendment to the Act on Register of Population and Birth Numbers entrusted the Office with competence in the area of administrative punishment, namely punishment of administrative delicts consisting in unauthorized management or use of birth numbers. The birth number (a national identifier in the Czech Republic), its use and utilization was subjected to legal regulation for the first time since its introduction. The Act currently stipulates who (which entity) is authorized to use birth numbers, either generally, as an institution, or on the basis of a special law. Where this statutory authorization does not exist, birth numbers may be used only with the consent of the relevant bearer or his statutory representative, as appropriate. The Act stipulated a relatively long transition period (one and a half years) to enable the individual users to adapt to the new statutory limits. The number of enquiries and requests for interpretation of the relevant provisions attained such volume that it was necessary for the Office to draw up, in cooperation with the entity submitting the amendment to the Act, the Ministry of Interior, a general application position, which was published in the Journal of the Office (No. 34/2004) and provided to the general public on its website. Nevertheless, the trend from previous years further continues and the birth number is often requested from the citizens also for a number of purely private acts and the consent to its use is, de facto, coerced, often under a concealed threat of non-provision of the offered service, if the birth number is not disclosed. Problems with interpretation were also caused by the fact that while a number of special laws permit the use of the birth number for identification, this is, e.g., only an alternative to the date of birth. Where the legislator used the wording "date of birth or birth number", and there are a great many regulations using this phrase, the new regulation of utilization of the birth number unambiguously gives the discretion to choose the type of data (i.e. either the birth number or the date of birth) to the bearer thereof. This has caused problems to those major controllers of personal data who have based their records on the identifier. Such controllers of personal data must adapt their records by the end of 2005 in that, unless they can base their use of birth numbers on a certain law or unless they have obtained the consent of the bearer of the number to its further use, they must demonstrably remove birth numbers from their records.

The amendment to the Act on Register of Population and Birth Numbers thus introduced a fundamental change in the potential for use of the personal identifier, in accordance with the general principles of protection of privacy.

Another, entirely new issue related to application of law by the Office, consists in its new competence based on Act No. 480/2004 Coll., on Certain Information Society Services and on the Amendment to Certain Other Acts.

The Act transposes to the legislation of the Czech Republic directive 2000/31/EC on Electronic Commerce, with respect to the Directive on Privacy in Electronic Communications, which emphasizes in its Article 5 the duty of the

Member States of the European Union to ensure confidential character of communications transferred through a public communication network and publicly accessible electronic services.

The Act is conceived as technically neutral and addresses part of a major issue, which has recently become increasingly important, i.e. "spamming". The Act regulates dissemination of commercial communications and consistently introduces to the Czech legislation the "opt-in" principle, i.e. the rule that a commercial communication may be sent by electronic media only with the prior consent of the addressee.

During the year, the Office was contacted by a number of persons, both natural and legal, with enquiries related to application approaches and interpretation of the Act. After publication of the Act in the Collection of Laws and its entering into effect at the beginning of September 2004, the number of requests for interpretation increased several times. The Office provided consultations, not only individually, on the basis of written and telephone enquiries, but its employees, together with representatives of the Ministry of Informatics, also provided the relevant explanations and comments at a number of lectures and workshops. The Office provided considerable amount of information through its website in the framework of the on-line open discussion forum. Information is also permanently published at this website, including the opportunity to raise complaints by this means.

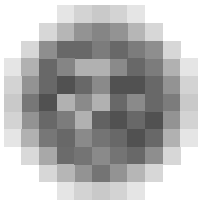
In general, it can be stated that, by unambiguously preferring the opt-in method for communication with customers, the Act on Certain Information Society Services and on the Amendment to Certain Other Acts is slightly stricter than the legal framework of EU. Through this Act, the legislator clearly and strongly advised all entities active in this area of its future intentions. In this case, it will defend, not only the privacy of natural persons, but also the right of legal persons "not to be bothered" by unsolicited electronic communications of the defined type.

Several judicial proceedings involving the Office as a party to a suite, were closed during the year. Four disputes concerning the competence to make a decision, where the matter was referred to the Office by general courts, were decided by the Special Senate of the Supreme Administrative Court in that the Office for Personal Data Protection, rather than the general courts, was competent to resolve the given matters, even though they were concerned with indemnification for nonproprietary damage. This decision was based on "gaps" in legislation. The Special Senate of the Supreme Administrative Court filled this gap by its interpretation. However, similar disputes can no longer arise, as the amendment (No. 439/2004 Coll.) to the Personal Data Protection Act clearly referred this subject to proceedings before the general courts.

A decision has also been made on a constitutional complaint lodged by the Czech Statistical Office in 2002 in relation to the prohibition to process certain personal data obtained during the census of the population, houses and apartments. The Constitutional Court rejected the complaint and it thus holds, that CSO may no longer use certain data from the census and these data are permanently blocked.

Three decisions on imposing a penalty were challenged by an administrative action. Two actions have already been decided by a senate of the Municipal Court in Prague in favour of the Office for Personal Data Protection (at the time of preparation of this Report, these decisions had not yet come into legal force); the court found no defects in the procedure of the Office for Personal Data Protection in imposing the penalties and fully upheld its legal argumentation.

It can thus be summarized that, in 2004, the Office for Personal Data Protection successfully followed-up on the high standard of application of law from the previous years. This was also positively reflected in spontaneous evaluations by citizens and legal persons, which the Office received in the form of letters of thanks.



Foreign Relations and Participation of the Office in International Cooperation

The contents and organization of foreign relations, including participation in international cooperation, is legislatively based particularly on the provisions of Article 29 (1) (g) of the Personal Data Protection Act, according to which the Office ensures fulfillment of requirements following from international treaties binding the Czech Republic. Another basic provision of the Act consists in Article 29 (1) (i), which obliges the Office to cooperate with similar authorities in other countries, with institutions of the European Union and with bodies of international organizations operating in the area of personal data protection; in addition, in accordance with the law of the European Communities, the Office must meet the obligation of notification towards the institutions of EU.

The European Association Agreement was the decisive international treaty up to the date of accession of the Czech Republic to EU; this Agreement imposed on the Office the duty to provide for harmonization of the national legislation and the related practice with the law of the European Union, the acquis communautaire, in the area of its competence. The main "pre-accession" documents of the European Union, such as the Comprehensive monitoring report on the state of preparedness for EU membership of the Czech Republic and other documents, appreciated the high degree of preparedness for accession in the area of protection of personal data. Simultaneously, they noted the need of certain "tuning" of the national legislation to Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and also the fact that ensuring of sustainable functioning in the long term requires supplementation of the personnel through additional recruiting. While it has not been possible to enforce any substantial increase in the human resources (in spite of new areas of competence of the Office), full transposition of the Directive through amendment to the Personal Data Protection Act has been completed. The Office ensured the transposition already in September 2003; however, given the prolonged legislative process, the relevant amending Act, No. 439/2004 Coll., entered into effect only as of July 26, 2004.

Both the Treaties establishing the European Communities and the European Union and all secondary law, including binding legal acts in the framework of acquis communautaire (regulations, directives and decisions), Convention No. 108 and other legislative rules valid for the 3rd Pillar of EU, have been fully applicable since the accession to the European Union. Two directives of the European Parliament and of the Council and several subsequent decisions of the European Commission have fundamental importance for protection of personal data in the Czech Republic. The above-cited documents include aforementioned Directive 95/46/EC and also Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); the decisions of the European

Commission are mostly related to the adequacy of protection of personal data in some third countries.

By the end of 2004, both the Office and the Czech Republic fully harmonized the legislation and practice with all legal acts under the acquis relevant for transposition, except for Directive 2002/58/EC. A certain part of this Directive, concerned with prohibition of unsolicited commercial communications (such as e.g. direct-marketing spams, etc.), was implemented in the framework of Act No. 480/2004 Coll., on Certain Information Society Services and on the Amendment to Certain Other Acts, with effect as of September 7, 2004. However, a vast majority of the contents of the Directive is yet to be implemented in the national legislation. The transposition, not only of this, but also of a number of other Directives within the "telecommunication package", should be ensured by the draft new Act on Electronic Communications, which was submitted by the Ministry of Informatics after prolonged and difficult preparations, which also involved the Office in the relevant stage. At the end of the monitored period, the Act was subject to a similarly difficult legislative process in the Parliament of the Czech Republic and its entry into force is not expected before January 2005.

Convention of the Council of Europe No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (ratified by the Czech Republic in 2001 and extended in 2003 to include non-automated processing of data and ratification of the Additional Protocol regarding supervisory authorities and transborder data flows), which was adopted by EU in the sphere of justice and home affairs, i.e. the above-mentioned 3rd Pillar, is also important for the area of protection of privacy. The Convention constitutes the basis of legislation applied within cooperation of the Czech Republic with Europol and in preparation for cooperation in the Schengen area, in which the Office very intensively participates, as also mentioned below.

The most important working platform for the relations and cooperation with both the European Commission and the partner supervisory bodies in other EU countries is the Article 29 Data Protection Working Party established under Article 29 of Directive 95/46/EC (WP 29). This is a renowned body of the European Commission with an advisory and independent status, whose meetings involve high-level representatives of independent supervisory bodies, usually presidents of the relevant authorities. Its meetings, even at the time before accession of the Czech Republic to EU, when representatives of authorities from the candidate countries had an advisory status, were of great importance with respect to obtaining information on fundamental documents in the area of data protection and the opportunity to "be heard" in the discussions. After accession to EU, the representative of the Office has been able to participate, as a fully-fledged member of the Working Party, in preparation of documents and standpoints with full power of his vote and thus affect the creation of EU policies in the given area. In 2004, the President of the Office participated in a total of six meetings of WP 29. The most important discussed documents included, e.g., the standpoints on transferring personal data of air passengers from the PNR systems (Passenger Name Record) to the U.S., Australia and Canada, on processing of personal data by means of camera monitoring, and on unsolicited communications for marketing purposes, the working document on genetic data, the standpoint on incorporation of biometric features in residence permits and visa documents in relation to the VIS system, etc.

In addition to the WP 29 platform, an opportunity to pursue close relations and ensure joint addressing of issues of the Office with the competent workplace for data protection of DG Internal Market of the European Commission is also provided by participation in the meetings of the Committee for Personal Data Protection established by Article 31 of Directive 95/46/EC (Committee 31), with

which the European Commission consults all decisions and measures in the area of personal data protection. If the adopted measures are not in accord with the standpoint of Committee 31, notice of this fact must be provided to the Council, which can then adopt a different decision. In 2004, the representative of the Office participated in three meetings of Committee 31. The most important discussed topics included evaluation of adequacy of personal data protection in some "third" countries in case of transfer of these data from the EU Member States and, e.g., draft "alternative standard contractual clauses" for the transfer of personal data to third countries, submitted by the business sector, etc.

Employees of the Office were also actively involved in the work of the International Working Group on Data Protection in Telecommunications, which engages in the area of personal data protection in connection with modern technology.

Inter-sectoral cooperation of the Office in relation to EU, and namely the Council/Coreper, is very intensive particularly with the Ministry of Informatics of the Czech Republic, which is also true with respect to the above-mentioned preparation of new laws. Collaboration with the Ministry of Informatics of the Czech Republic is concerned, e.g., with the area of information society, regulation from the viewpoint of data and electronic communications security, establishment of information systems of public administration (e-Government), regulation in the provision of services connected with public electronic networks, etc.

Close cooperation with the Ministry of Interior of the Czech Republic in the framework of the aforementioned 3rd Pillar of EU, particularly in relation to preparation for accession to the Schengen Convention, which presupposes creation of the National Schengen Information System (NSIS) with connection to the international Schengen information system, is another example. This preparation required participation in a number of undertakings and activities coordinated by the Ministry of Interior. However, the future full performance of the supervisory powers in the framework of the 3rd Pillar is inconceivable without an increase in the human resources of the Office. These activities will include, not only supervision over the related national activities of the Police of the Czech Republic and other national bodies, but also fully fledged participation in activities of the Joint Supervisory Authority of Schengen (JSA), where the representatives of the Office are currently invited as observers. On the basis of accession to the Europol Convention, the authorized employees of the Office, as full members, already participate in the work of the Joint Supervisory Body of Europol (JSB) and, on the basis of accession to the Convention on the Use of Information Technology for Customs Purposes, also in the work of JSA Customs. At the 31st meeting of JSB Europol on December 20, 2004, an inspector of the Office, PhDr. Miroslava Matoušová, was elected for a term of 3 years as a Vice-Chairman of this body.

Joint activities of representatives of supervisory bodies in the area of data protection from the countries of Central and Eastern Europe and Baltic countries, commenced in 2001 on the basis of an initiative of the Czech Office and the Polish Office of the General Inspector for Personal Data Protection, also continued in 2004. These activities have the form of working meetings (Riga, May 13 – 14, 2004) and other contacts, including communication with the use of common website (www.ceecprivacy.org).

From the viewpoint of bilateral relations with the partner supervisory bodies of other countries, the Office has established long-term above-standard cooperative relations with the Spanish Data Protection Agency.

In late April 2004, the Office, together with its Spanish partner, concluded eight-month cooperation in implementation of the project entitled "Enforcement of Data Protection Acquis". This "twinning-light" project with reference number CZ01/IB/OT-01-TWL, which was financed from the Phare funds, was commenced

in September 2003. It provided an opportunity for exchange of knowledge and experience in the area of personal data protection, with special respect to electronic communications and special databases established in the European Union in the framework of the Schengen cooperation, Europol and the Customs Information Systems. Four working meetings between the two partners took place in Prague during fulfillment of the objectives of the project. At this occasion, the Spanish party also provided experts for three topical workshops, which involved, in addition to employees of the Office, also experts from selected governmental institutions and private corporations. The experts of the Office could also increase their knowledge during three study visits in the Madrid headquarters of the Spanish Agency. This project, which was the second Phare project implemented by the Office together with the Spanish Agency, provided considerable assistance to Czech data protectors in their attempts to achieve European standards in specific areas, such as electronic communications and databases established in the framework of international police and customs cooperation. Successful completion of this project improved the good relations between the Czech and Spanish parties, whose basis was established already during implementation of the previous Phare twinning project in the 2001-2002 period.

In cooperation with the Spanish Agency, the Office responded to the invitation of EU, which was seeking for a suitable leader of the CARDS project (similar to Phare projects, but aimed at the former Yugoslav countries) intended for support for Bosnia and Herzegovina in the creation of a legislative and institutional basis of personal data protection with emphasis on the 3rd Pillar. If the Czech-Spanish offer is accepted, the project, involving, in addition to organization of workshops and working meetings, also a long-term stay of an expert of the Office at the beneficiary of the assistance, will be commenced in 2005.

Participation in regular meetings of experts, mainly experts on control and inspection activities, concerned with addressing complaints of citizens, contributes to development of working contacts with the partner supervisory authorities from other EU countries. On November 4-5, 2004, the Office organized the "10th Complaints Handling Workshop" in Prague. Simultaneously, its experts participated in at the high professional level of this meeting through their lectures and presentations (Ing. J. Zapletal, JUDr. V. Bartík, JUDr. J. Maštalka, Mgr. J. Prokeš, PhDr. H. Štěpánková).

The continuing participation of the Office in activities following from the obligations of the Czech Republic as a member state of the Council of Europe and OECD is also related to fulfillment of the requirements of the international agreements.

The President of the Office represented the Czech Republic for a number of years in the Council of Europe in the project group on data protection (CJ-PD) and was also an elected member of the coordination committee (CJ-PD/CG). The President participated in the long term in creation of documents of the Council of Europe in this area and has been entrusted with creation of documents on the protection of personal data in the use of chip cards. At the end of 2003, the CJ-PD working group terminated its activities and its agenda was transferred to the Data Protection Committee established pursuant to Convention No. 108 (T-PD), which is the supreme body of the Council of Europe dealing with data protection; at this occasion, the President of the Office was elected first vice-chairman of T-PD.

On October 14-15, 2004, the Council of Europe, in cooperation with the Office, organized an international conference entitled "Rights and Responsibilities of Data Subjects" in Prague. This prestigious undertaking, which was the most important of international events ever organized or co-organized by the Office, involved 66 participants from 33 countries and 3 international organizations. The conference was held under the auspices of the Minister of Foreign Affairs, Mr. Cyril Svoboda. The Chairman of the Senate of the Czech Republic, Mr. Petr

Pithart, greeted the conference through an introductory word in presence of important persons – Ambassador of the Czech Republic to the Council of Europe, Ms. Vlasta Štěpová, the European Data Protection Supervisor, Mr. Peter Hustinx, and the General Director of Legal Affairs of the Council of Europe, Mr. Guy de Vel.

In the framework of OECD, cooperation is continuing with the Working Party for Information Security and Privacy (WPISP under the ICCP committee). The special importance of the OECD platform and events organized by it lies in the acquisition of valuable information on approaches to data protection outside Europe and on the potential for employing self-regulating tools in the given area, such as codes of conduct, alternative resolution of disputes, privacy enhancing technologies, etc. An important contribution of OECD is anticipated in relation to the very sensitive and topical issue of seeking a balanced approach to the legitimate attempts to increase security in relation to the growth of terrorism, on the one hand, and protection of democratic values, such as the right to privacy, on the other hand. An important contribution is the introduction of the term "culture of security" connected with elaborated principles of the newly conceived Security Guidelines in the area of information.

Relations of the Office with other countries and the consequent participation in foreign events were substantially developed, e.g., in the area of solutions connected with implementation of Directive 2002/58/EC, the issue of dissemination of commercial communications, legal and technical questions of electronic communications, and issues in the use of biometric data. Interest was also concentrated on international discussions on the effectiveness of control activities and supervisory processes in personal data protection. The interest in findings related to personal data protection in police and customs services was based both on new commitments of the Czech Republic assumed in relation to the accession to the relevant conventions (Europol, customs affairs) and on the preparation for future tasks, which will need to be addressed by the Office after accession of the Czech Republic to the Schengen area.

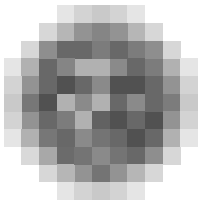
The 26th International Conference of the Commissioners for Privacy and Personal Data Protection "The Right to Privacy – The Right to Dignity" (Wroclaw, September 14-16, 2004) was an example of important events, in which the responsible employees of the Office actively participated. Within the Conference, the President of the Czech Office led a panel concerned with the issues of security in the use of biometric data. Through their lectures and presentations, a number of experts of the Office also substantially contributed to the meeting of EPON – European Privacy Officers Network, held in Prague on November 2-3, 2004, to which representatives of the personal data protection authorities of the Czech Republic, Poland and Hungary were invited. The presentations of the representatives of the Office were concerned with incorporation of personal data protection in the national legislation and practice and the expected changes in further development of personal data protection (RNDr. Karel Neuwirt), the policy of transferring personal data to countries outside EEA (Ing. Ivan Procházka), the policy of direct and indirect marketing (Mgr. Josef Prokeš), the policy of monitoring persons at workplaces (JUDr. Václav Bartík), and the policy of law enforcement (JUDr. Jiří Maštalka).

Representatives of the Office participated in a number of foreign undertakings through their lectures or chairing panel discussions, including:

- The European Privacy Officer's Forum – EPOF (Brussels, January 27, 2004, President of the Office);
- 2nd European meeting of the Enterprise Privacy Authorization Language – EPAL (Lübeck, May 13-14, 2004, PhDr. Miroslava Matoušová);

- Biometrics and the Benefits to the Citizens (EU Summit, Dublin, May 14-15, 2004, President of the Office);
- Public Voice Symposium EPIC (Wroclaw, September 13, 2004, President of the Office);
- "ISSE 2004" Conference (member of the Program and Scientific Committee, Berlin, September 28-30, 2004, President of the Office);
- Workshop "Public Sector Data Sharing" (British Institute of International and Comparative Law, London, November 16, 2004, President of the Office).

A number of foreign experts from partner supervisory bodies (Poland, Slovakia, Spain) visited the Office in 2004. An invitation to visit the Office was also accepted by experts from Australia, who visited the Office after the end of the global conference in Wroclaw and presented interesting lectures within meetings with selected employees. Mr. Paul Chadwick, the Privacy Commissioner of Victoria (Melbourne) visited the Office on September 2004, and Mr. Paul Armstrong, the Director of the Legislative and Legal Department the Office of the Federal Privacy Commissioner in Sydney, visited the Office on September 24, 2004. The lectures contained information on practical legislative experience in the area of privacy protection in Australia, namely, e.g. with emphasis on raising the general awareness of protection of privacy, development of the relevant Australian legislation and specific features compared to Europe.



The Office, Media and Means of Communication

The trend of media interest in personal data protection, which was noted by the Office already during the previous year, increased in 2004: This is an interest that can easily be described as permanent and consistent. It follows from evaluation of monitoring of the media that the subject of personal data appears, on average, in ten reports every day. Therefore, it can be stated in general that this relatively new dimension in the life of the democratic society receives continuous attention. However, this does not mean that the published reports are always correct and competent in issues of personal data protection and that interpretation of the Personal Data Protection Act is not sometimes misleading or even controversial. The Office responds to these situations and pays attention to them at its regular press conferences in an attempt to clarify the principles of protection of personal data, scope of the Personal Data Protection Act in the framework of the Czech legislation and in relation to the European legal rules and documents.

Substantially more reports are regularly concerned with cases including suspicion of violation of the Personal Data Protection Act, which are, de facto, initiated by a finding of a certain media.

The situation in the media always substantially changes after the regular press conferences of the Office, particularly with respect to the number and also correctness of the published reports.

The table provided at the end of this Chapter clearly illustrates the contacts of the Office with the media, particularly from the quantitative viewpoint. There was a clear increase compared to the previous year (by more than 100 cases).

PRESS CONFERENCES

From the temporal viewpoint, it could be stated that the regular quarterly press conferences of the Office substantially affects the attention paid by the media to personal data protection: it is statistically demonstrable that the number of reports substantially increases during the first 3 days after press conferences. 66 to 119 reports concerned with the issue of personal data was published during this period in 2004. A similar situation occurred after the press conference held by the Office during the Prague conference called “Rights and Responsibilities of Data Subjects” organized by the Office under the auspices of the Council of Europe: 59 reports were published during the subsequent three days.

At the present time, after four years of existence of the Office, press conferences can also be described with respect to their course: they usually have not only informative nature, but also include a discussion enabling to provide more thorough knowledge on personal data protection, which is carefully followed and actively instigated by journalists for over than hour. Therefore, in 2004, the Office reserved a certain part of press conferences for more thorough insight into a specific area of working duties of the Office and the related legal impacts (at the time

of finalization of the amendment to the Personal Data Protection Act, attention was paid, e.g., to the work of the Department of Legal Affairs and the issues addressed by the department; at the time of establishment of the new Administrative Proceedings Department, this department was introduced and discussion was held on punishment and sanctions; the next topic was related to the control activities – in connection with the newly established Article of Control and Administrative Activities of the Office, etc.).

PUBLISHING ACTIVITY OF THE OFFICE AND DISSEMINATION OF NEW EUROPEAN AND GLOBAL FINDINGS IN THE FIELD OF PERSONAL DATA PROTECTION

OTHER COMMUNICATION PROCEDURES

In 2004, the Office issued 6 editions of the Journal (Nos. 30 to 35) in a total number of 3750 copies. On the basis of the amendment to the Personal Data Protection Act, a change was made during 2004 in the publication of the Journal, whose periodicity was based on the statutory duty to publish newly registered controllers of personal data within two months of registration: the Office is now obliged (as follows from Article 35 (3) of the Personal Data Protection Act) to publish in the Journal cancellation of registration pursuant to Article 17 of the Act. This information is published in the section Registrations of the Journal (a survey of registered entities is now published exclusively on the website of the Office).

Similarly, the sections Positions of the Office and Communications of the Office continue to be published in the Journal. A new section entitled Materials from the Official Journal of the European Union was established after accession of the Czech Republic to the European Union; this section includes copies of European documents that are relevant from the viewpoint of personal data protection and privacy of citizens.

The Journal of the Office continued to be published by SEVT, s.r.o. in 2004.

The Information Bulletin of the Office is now published quarterly. The Office considered it necessary to provide the last edition of 2004, given the extensive scope of published materials, to the general public and published it as a double edition (3-4).

In 2004, the bulletin has changed with respect to its composition, particularly from the viewpoint of the published foreign materials: a relatively large space is devoted in each edition to one topic discussed abroad; its choice is determined particularly by issues topical in the Czech Republic or the frequency of enquiries concerning the given issue, which was recorded by the Office. In 2004, such topics included camera monitoring systems, as this issue raised a considerable interest of the public and the media, undoubtedly also in relation to the uncertainty following from the absent legislative regulation of this means, whose utilization is continuously increasing.

The bulletin, whose printing and distribution is still ensured by the Office from its own resources and means, is a source of information and, based on certain statements, also of reference, whose use constantly increases. Its edition of 450 copies probably no longer suffices to satisfy the public interest. Therefore, it is a task for the next year to undertake the relevant survey in this sense and, in accordance with its results, provide for the required edition of the Information Bulletin.

The website of the Office provides large amount of information (which was documented by the recently published media evaluation of websites of governmental agencies). In 2004, this information was updated, particularly in relation to the establishment of the Department of Administrative Decision-Making and to the adoption of the Act on Certain Information Society Services and on the Amendment to Certain Other Acts, which entrusted the Office with competence in the area of punishment of

unsolicited commercial communications. From amongst foreign materials, fundamental documents of the Article 29 Data Protection Working Party established under Article 29 of Directive 95/46/EC are also newly published. After approximately 3 weeks from distribution of the Journal, the materials published in the Journal are included in the relevant sections of the website.

A new graphic design of the website was prepared and their structure updated during the year. New design of the website should be introduced in 2005.

In 2004, the Office offered to the general public the option of putting forth electronic enquiries through an open on-line discussion forum on the website in connection with the new competence entrusted to the Office by the amended Act on Register of Population and Birth Numbers and in connection with punishment of dissemination of unsolicited commercial communications.

In 2004, the Office also sent two of its positions in electronic form directly to municipal authorities. These positions included legal analyses of situations, which the Office considered to be especially relevant for these authorities: the first position was drawn up in cooperation with the Ministry of Interior and was entitled "Disclosure and Publication of Personal Data from Meetings of Boards and Councils of Municipalities and Regions" and the second position was concerned with "Keeping Records in Entry to Buildings". A very extensive database established by the Office for the purpose of communication with cities and municipalities is utilized exclusively on the basis of interest shown by the relevant body in the disseminated materials. It should be noted that this service was refused only in a single case.

Publishing activities of the President, inspectors and lawyers of the Office continued in 2004. Lectures provided by employees of the Office, which are subject to considerable interest, even had to be strictly limited given the increasing workload of the Office following from the newly entrusted competence.

The book of Ms. M. Matou_ová (inspector of the Office) and coll. entitled "Protection of Personal Data", which was published in the last quarter of 2004 (ASPI publishing house) will undoubtedly become an important source of information with respect to protection of personal data.

A meeting with the representatives of the City Ward Prague 7 was held at the Office in March 2004, which developed into a very intensive and mutually beneficial three-hour discussion with the Municipal Authority of Prague 7, in whose jurisdiction the Office has its seat. Cooperation was thus initiated, which will further continue, inter alia, by a meeting with the citizens. The meeting confirmed that cooperation with the representatives of self-governing bodies provides new opportunities for disseminating knowledge on personal data protection and a valuable feedback for the Office.

In late 2004, the Office finalized an information leaflet intended for acquaintance of the citizens with the basic principles of personal data protection and with their rights to protection of privacy. The leaflet will be printed in January 2005 in an edition of 200 000 copies and will be distributed to the municipal authorities of cities, authorities of city wards and districts and also municipal authorities in the entire territory of the Czech Republic.

LIBRARY OF THE OFFICE

In 2004, the library provided its on-the-spot services in full scope, as originally conceived. The Clavius library system, introduced in 2003, was also put into routine daily operation.

The library continues to purchase books relevant for the given sector, concerning directly personal data protection or the related issue of protection of human rights, both in Czech and in English, and basic literature from the areas of

law and legislation; and creates a sectoral fund of European legal rules and documents; collects legal literature – inter alia, sectoral dictionaries. It is also appropriately equipped with encyclopedias, explanatory and language dictionaries, and, to a small degree, also Czech historical literature mapping the development of the European civilization and law, publications providing insight into the issue of new information technologies regarding data protection and protection of human rights.

The library has also periodicals with similar focus. During the year, it extended its fund in a very economic manner – it was extended by 187 items. Nevertheless, it also has available a number of foreign publications, which it obtains from its partner organizations both in Europe and overseas, including annual reports of these institutions, outputs and proceedings from conferences and workshops concerned with data protection.

Employees of the Office can also use the services of the library through the Intranet – information is published on newly acquired books. Information on the contents of newly received periodicals are also processed and provided through the Intranet and, in the form of more extensive annotations, reports are provided on articles in English periodicals.

Adequate space and technical background available to the library allowed for its use also by external persons; these persons included university students from both Prague and outside Prague, in particular, students of law, and also students of secondary vocational schools – those, who sought basic documents for their theses concerning personal data protection. Naturally, in this context, they also received the necessary consultations from the employees of the Press Department and from other employees of the Office, as appropriate. Six theses were thus drawn up during the second half of 2004 with support from the Office. The library also provided its services to the Slovak partner authority. In this sense, the library already fulfills its originally contemplated tasks.

The Office has provided a possibility of a three-week assignment to a student of the 2nd year of the Secondary Vocational School for EU Administration; it allowed her, inter alia, to participate in arrangement of the above-mentioned conference organized by the Office on the basis of authorization by the Council of Europe.

OTHER INFORMATION FUNDS

A video archive of the Office was created on digital carriers during 2004. The efficient and purpose-driven topical classification enables to monitor the history of media activities of the Office in relation the issue of personal data protection in the Czech Republic, including problems that are and have been subject to media attention, often in response to instigations of the general public. In addition to an archival value from the viewpoint of history of personal data protection in the Czech Republic and the Office itself, the archived items can also serve for the employees of the Office as basic documents or sources, e.g., when handling current cases. The archive currently includes 86 items classified according to their subject.

The task for 2005 will be to ensure the same arrangement of audio materials that have been gathered in a considerable number by the Office during the four years of its existence.

The fund of visual communication, which is being created by the Office, is also rare and very interesting: it consists of a collection of posters that were used for conferences throughout the world and for professional workshops of data protection authorities or are related to these topics and were issued by the Council of Europe or supervisory data protection institutions in the world.

The collection markedly vitalizes and decorates the common premises and corridors of the Office, accessible to both its employees and visitors. This lively, i.e. continuously supplemented, and unique undertaking was also noted by foreign guests of the Office.

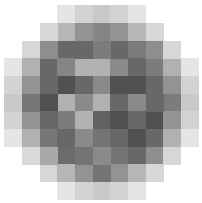
In 2004, the above-mentioned visual fund was enriched by a Czech contribution: a set of posters created at the occasion of the previously mentioned conference "Rights and Responsibilities of Data Subjects". Through the posters, the Office intended to promote the importance of the conference, which was held by the Council of Europe for the first time in a new Member State of EU; the conference was also considered to be the most important international activity ever organized by the Office.

In the context of this project, the Office again successfully cooperated with the graphic design and visual communication atelier of the Academy of Arts, Architecture and Design (in 2003, this atelier created the logo of the Office); the design of the set of posters was created, under professional guidance by Doc. Rostislav Vaněk, by a student of the 2nd year, Michal Kopecký, and the Academy also partly ensured printing of the posters. The Council of Europe intends to use a fragment of one of the posters on the cover of the proceedings from the conference. The poster has beeen used as a figure in the chapter Foreign Relations and Participation of the Ofiice in International Cooperation.

COMMUNICATION OF THE OFFICE WITH MEDIA IN FIGURES:

Period: January – December 2004

Agency service	26
Press total	168
Daily press	131
Other periodicals	37
Television	56
Radio	38
Basic documents for the media	66
Media total	354



Administration of the Information System

In 2004, the Department of Informatics concentrated its activities, not only on maintaining fluent operation of the information system of the Office, but mainly on further development of the entire system from the viewpoint of modification of the current program applications and introduction of new applications. Considerable efforts were again exerted during the year to improve the protection against unfavorable penetration into the system and attack of viruses.

An amendment to the Personal Data Protection Act introduced substantial changes in the process of registration of entities processing personal data, which directly affected the program application used in this context.

On the basis of new Act No. 480/2004 Coll., on Certain Information Society Services and on the Amendment to Certain Other Acts, the Office was entrusted with a new area of competence in the field of supervision and assessment of unsolicited commercial communications disseminated through electronic means.

These facts, together with the increasing workload of the Office and its internal reorganization, required a strategic decision on modification of the information system used by the Office.

A decision was made on a fundamental upgrade of the filing service and its extensive use in the Office. The software applications used by the Office are gradually modified, both from the viewpoint of new functions related to legislative changes and from the viewpoint of a new version and introduction of the filing service. These fundamental changes also affected work on the prepared module Control activities of the Register application.

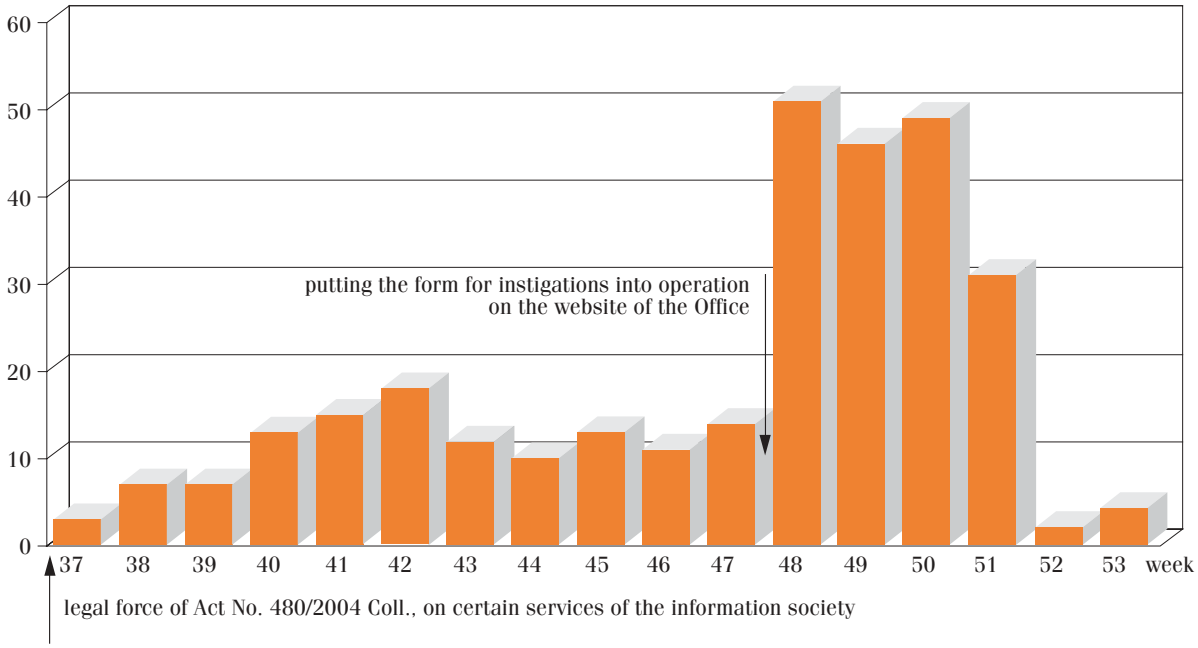
In addition to the above-mentioned change in the information system, it was necessary to solve performance of new competences in the area of unsolicited commercial communications, following from Act No. 480/2004 Coll. As this is an entirely new task, its fulfillment was divided to several gradual steps. The first step included creation of an information system for collection of instigations regarding this type of intrusive correspondence. A form allowing for straightforward submission of instigations was prepared and put into operation on the website of the Office. Another step consists in the preparation of an application for processing the instigations. This application is also directly connected with the information system of the filing service.

In cooperation with the main supplier of the information system, the employees of the Department of Informatics managed, in addition to the complex developmental tasks, to provide for every-day functioning of the entire information system of the Office, including all user stations, the network structure and office, communication and security technology, even under very complicated conditions during construction work in the building of the Office. In addition, they built a computer teaching room and gradually provided user training for employees of the Office in the area of use of computer technology. They also newly prepared the guidelines entitled “Principles of use of computer, office, communication and audio-visual equipment and work with the information system”.

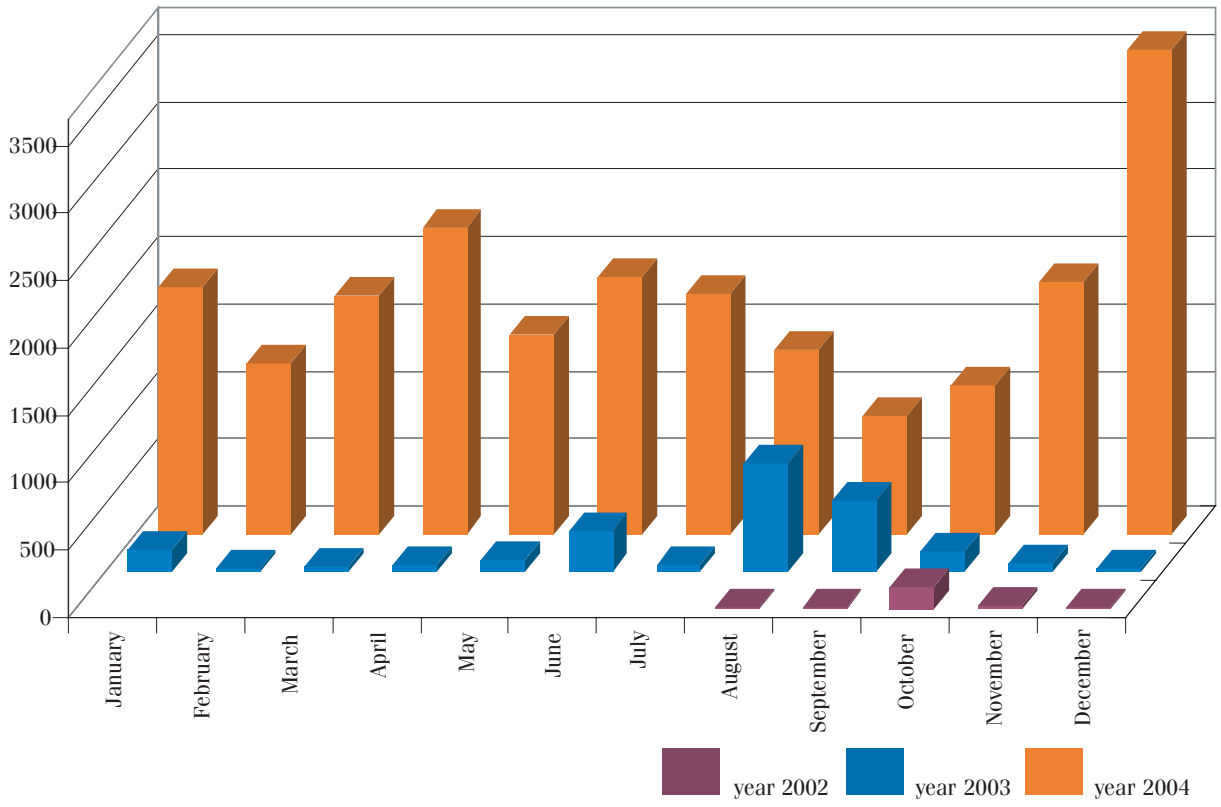
Under the pressure of constantly increasing danger of viral infection, in particular, of the e-mail system, the entire information system was equipped with a second anti-virus product of a different producer so that the combination of two independent products increased the security of the system and particularly the timely provision of new updates of the database of viruses. Simultaneously, this additional line of defense was supplemented by search for viruses in internet communications and by an anti-spam product containing both filters and heuristic analysis of e-mail messages.

With much more intensity than during the previous years, the employees of the Department of Informatics engaged in the work of international organizations (the Contact Network of Spam Authorities – CNSA attached to DG INFSO, which was established on instigation of the European Commission, and in the International Working Group on Data Protection in Telecommunication attached to Berliner Beauftragter für Datenschutz und Informationsfreiheit). The CNSA group consists of national authorities interested in implementation of Article 13 of Directive 2002/58/EC on privacy and electronic communications. The employees of the Department of Informatics participated in all meetings of this group and, on December 8, 2004, the Office officially accepted the Cooperation Protocol and is ready for active cooperation in the framework of this contact network. During the year, they also participated in the Symposium on Privacy and Security, organized by the Foundation for Privacy and Security, in the ISSE 2004 international conference (Information Security Solution Europe) and in the Workshop on RFID and its Impact, organized by the European Academy for Freedom of Information and Data Protection.

Number of accepted instigations related to dissemination of unsolicited commercial communications in 2004



Number of viruses and worms detected in e-mails



Personnel of the Office

Work was carried out during 2004 on preparation of a new organizational structure aimed at optimizing procedures in the performance of administrative activities and provision for the maximum effectiveness in the performance of control and administrative tasks. A new organizational department was established – the Article of Control and Administrative Activities of the Office – which should create a personnel, organizational and professional background for the performance of statutory competence of the Office.

The new organizational rules of the Office came into force on December 1, 2004. Thus, 2 organizational charts of the Office are depicted below: 1. The organizational structure valid until November 30, 2004, and 2. The organizational structure valid from December 1, 2004.

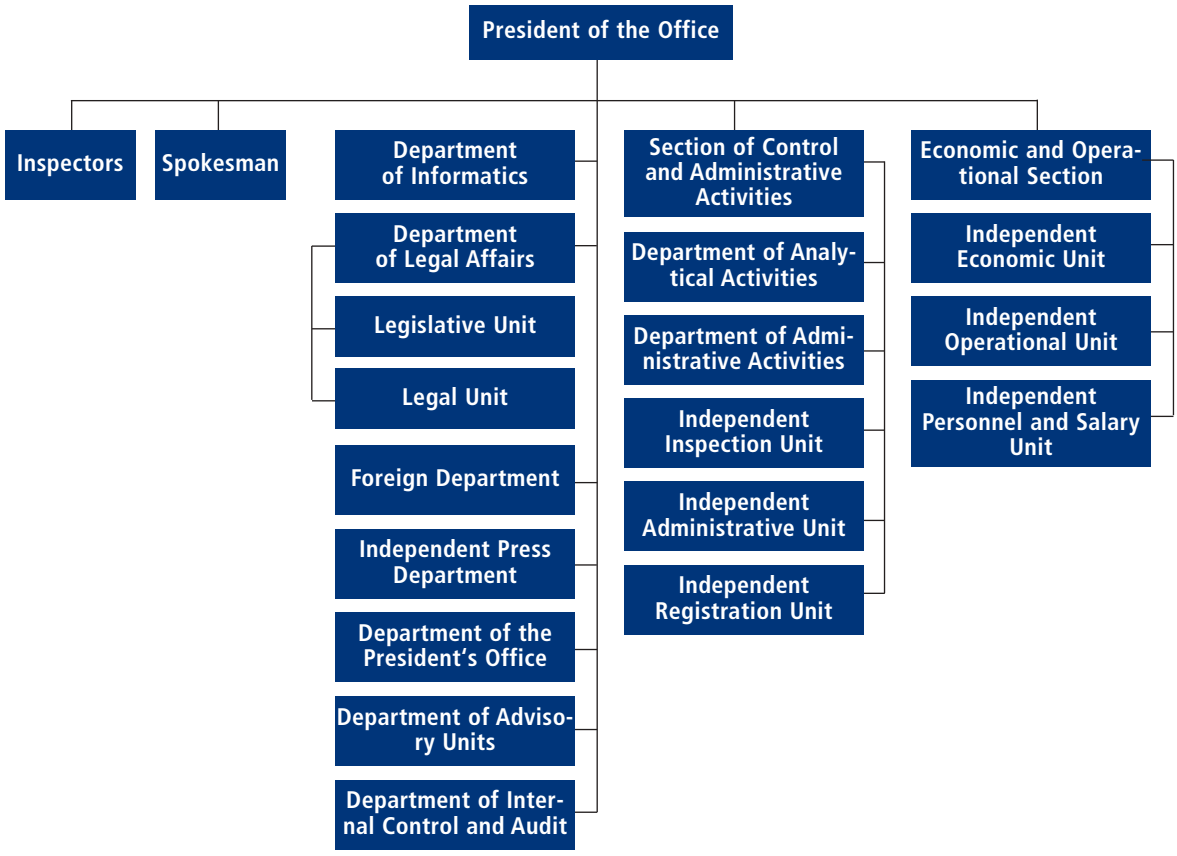
Given the new areas of competence entrusted to the Office during 2004, which extended the activities of the Office (competence to discuss administrative delicts consisting in unauthorized management of birth numbers and in unauthorized use of birth numbers; competence to perform supervision over compliance with the law in dissemination of commercial communications), analysis was carried out of the scope of work of the Office; it appears to be necessary to increase the number of workplaces in the Office.

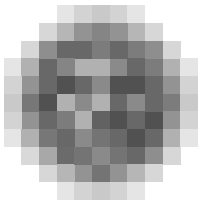
The future systemic arrangement concerning workplaces must be resolved in cooperation with the Government of the Czech Republic.

As of December 31, 2004 (January 1, 2005), the Office for Personal Data Protection had 74 (74) employees.

Organizational structure valid to November 30, 2004

Organizational structure valid from December 1, 2004





Economic Management of the Office

The budget of the Office was approved by Act No. 457/2003 Coll., on the state budget of the Czech Republic for 2004.

Withdrawal of Chapter 343 of the state budget – Office for Personal Data Protection

Summary indicators	in CZK thous.
Total non-tax and capital income and accepted subsidies	3 172,71
Total expenditures	208 027,33
Individual expenditure indicators	
Salaries of employees and other payments for performed work	25 540
of which: salaries of employees	24 937
other payments for performed work	603
Mandatory insurance premiums paid by the employer *)	8 488
Contribution to the Cultural and Social Needs Fund	493
Expenditures for financing programs pursuant to Schedule No. 5	120 597
of which: capital expenditures	112 452
non-investment expenditures monitored in ISPROFIN	8 145
Common non-investment expenditures and related expenditures	10 309
Transfer to the reserve fund	42 600
Specific individual indicators	0

**) premiums for social security and the contribution for the state employment policy and premiums for the public health insurance*
Note: The figures were adopted from statements drawn up as of January 31, 2005.

1. Income

Income was not classified within the budget for 2004. The total income of Chapter 343 - Office for Personal Data Protection equaled CZK 3,172.71 thous.

This income consisted of income for lease of non-residential premises to Stavební spořitelna ČS, refunds for foreign trips of employees of the Office from the Council of Europe and the European Commission, interest accrued in the account kept by the Czech National Bank and income related to 2003 (transfer of the balance of the deposit account after payment of salaries and the allocation to the Cultural and Social Needs Fund for December 2003).

The income account included the use of money from the reserve fund in a total amount of CZK 3 000 thous. p.a. for the purchase of a property required for establishment of an administrative building for the Office.

All income of the Office were transferred to the state budget.

2. Common expenditures

Withdrawals for common expenditures in an amount of CZK 10,309 thousand correspond to the common operational expenditures that follow from the main activities of the Office, including particularly items connected with purchase of minor tangible assets, materials, services, travel allowances, maintenance and expenditures related to non-investment purchases. The withdrawals also covered costs connected with organization and holding of the International Conference of the Council of Europe entitled "Rights and Responsibilities of Data Subjects" and the European workshop entitled "Addressing Complaints". Part of the costs in an amount of CZK 259.44 thousand was refunded by the Council of Europe.

The aforementioned amount corresponds to the requirement for purposeful and economic operation of the Office. The unused common operational expenditures in an amount of CZK 21,750 thousand were transferred to the reserve fund in accordance with Article 47 of Act No. 218/2000 Coll., as amended.

3. Salaries of employees and other payments for performed work

Financing from the budget of salaries of employees and other expenditures for the performed work correspond to the qualification structure and fulfillment of the plan by the employees.

As of December 31, 2004, the personnel consisted of 74 employees.

In accordance with the planned reduction of the number of systemic positions in the central governmental agencies in the 2004-2006 period, the headcount was reduced by 2 employees.

Salary funds in an amount of CZK 5,240 thousand, which were not as a consequence of not attaining the planned number of employees, were transferred to the reserve fund.

4. Expenditures for financing programs included in the information system of the Ministry of Finance - ISPROFIN

A total of CZK 120,597.34 thousand was withdrawn in accordance with the approved documentation of program 243 010 "Acquisition and renewal of the material and technical background for the Office for Personal Data Protection".

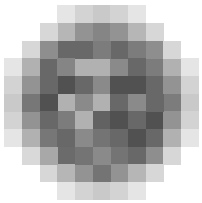
Of this amount, CZK 112,452.15 thousand were used for systemic investment expenditures. These expenditures included particularly individually evaluated investment expenditures connected with acquisition of an administrative building, in an amount of CZK 103,457 thousand, and with purchase of a property, in a n amount of CZK 3,043 thousand, with the use of means from the reserve fund, and also with the related construction work. Provision was also made for purchase of computer technology, two multi-functional printers and a set of sliding shelves for the archive. Furthermore, purchases were implemented with respect to an extension of audio-visual equipment for the conference and lecture room and supplementation of the camera system. Financial provision was also made for introduction of E-files, extension of the program equipment and improvement of protection of the information system of the Office.

Non-investment systemic expenditures were withdrawn in an amount of CZK 8,145.19 thousand and were used for payment of ICT operational costs, services and maintenance of equipment and minor tangible investment assets.

The unused investment systemic expenditures in an amount of CZK 260 thousand and non-investment systemic expenditures in an amount of CZK 15,350 thousand were transferred to the reserve fund in accordance with Article 47 of Act No. 218/2000 Coll., as amended.

5. Internal audit and internal control

The activities of the internal audit and functioning of the internal control system is fully based on Act No. 320/2001 Coll. Responsibility for internal audit is borne by an employee, who carried 3 audits in accordance with the annual plan, namely the audit of the procedure in drawing up the budget, audit of keeping records of insurance of the assets, and audit of public procurement. New implementing Decree No. 416/2004 Coll. was transformed to internal directive No. 7/2004. Internal control is ensured by all senior officers of the Office. The President of the Office was regularly informed of the results of internal controls in 2004. In most cases, minor shortcomings were promptly remedied; no material finding was made in the sense of Article 22 (6) of the Financial Control Act.



Provision of information pursuant to Act No. 106/1999 Coll., on free access to information

On September 29, 2004, the Office for Personal Data Protection received the 2nd prize in the "Open" category of the OPEN x CLOSED competition. The Office was awarded for exemplary provision of information for administrative proceedings. The results of the second year of the competition were announced by Otevřená společnost, o.p.s. (Open Society) at the occasion of the International Day of Information.

Re: Article 18 (1) (a)

In 2004, as in the previous years, the Office noted that enquiring persons often request information pursuant to Act No. 106/1999 Coll., although they, in fact, request interpretation of the Personal Data Protection Act or consultation related to the Personal Data Protection Act.

A survey of the extensive information activities of the Office following from the duties stipulated by Act No. 101/2000 Coll., as amended, is contained in the summary table on p. 9.

During 2004, the Office received 6 enquiries, which were denoted by the petitioners as enquiries pursuant to the Act on Free Access to Information.

In fact, only 2 of those enquiries were actually subject to that Act. The enquiries were answered in due time.

In other cases, the enquiries concerned issues regulated by Act No. 101/2000 Coll., on personal data protection, as amended, and were answered in the framework of normal consultations provided by the Office.

However, in all cases, the Office answered the enquiries within the deadlines stipulated by Act No. 106/1999 Coll., on free access to information.

Re: Article 18 (1) (b)

Not applicable in 2004.

Re: Article 18 (1) (c)

Not applicable in 2004.

Re: Article 18 (1) (d)

No proceedings on penalties were held.

Re: Article 18 (1) (e)

Not applicable in 2004.