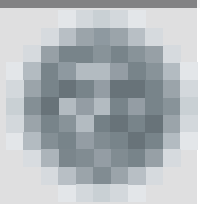
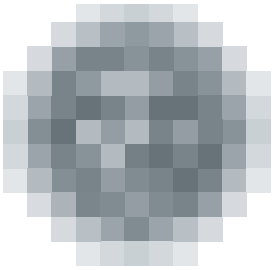
ANNUAL REPORT SUMMARY

2009



úřad pro ochranu osobních údajů
the office for personal data protection

ANNUAL REPORT SUMMARY 2009



úřad pro ochranu osobních údajů
the office for personal data protection

The president of the office looks back at 2009

The presented Annual Report provides primarily a detailed overview of the Office's control activities. However, given its concept, this report could serve not only as a summary document, but also as a detailed description of the Office's decision-making and its interpretation of the Personal Data Protection Act, where the competence of the Office also includes supervision of compliance. With slight exaggeration, I could say that this is a precedent of kind, which is also quite easy to understand for laymen. I consider this important particularly because the Office has been exerting consistent efforts to ensure that the Personal Data Protection Act and its links to protection of privacy are well understood by as many citizens as possible. For me, privacy is one of the fundamental values of our civilization and one of the basic preconditions for its preservation for future generations.

These efforts also encompass lectures provided by the Office and the three-year educational project entitled "Personal Data Protection in Education", which was accredited by the Ministry of Education, Youth and Sports in late 2006 and completed in 2009. A total of 211 teachers took part in a workshop organized by the Office within this project – some of them even returned with new inquiries; some educational facilities sent several employees and these were provided with a certificate of participation in the workshop. Their attitudes and appreciation gave us a feeling of a considerable accomplishment.

Last year, the Office also successfully undertook activities related to the Czech Presidency of the EU in the first half of 2009. These aspects are discussed in detail in the part of the Annual Report dedicated to the Office's foreign activities. In 2010 the Office will follow up on a number of new contacts and instigations.

Although we had to deal with a great many problematic cases of personal data processing during the year, which fact is also demonstrated by the contents of the chapters dedicated to the Office's control and administrative activities, I consider it especially important that we managed to make progress in at least two areas which the Office greatly emphasised last year: This is particularly true of the progress in elaborating legislation on the use of video surveillance systems, which should be completed in 2010. I also believe that the very extensive workshop devoted to the aspects of legislation on management of DNA profiles, which was held in the Senate under the auspices of its Vice-President

and the chairwoman of its Standing Commission on Privacy Protection, marked the first step on the path towards better legislative protection of one of the most intimate items of personal data, where infringement of privacy is absolutely fatal. I am realistic enough not to expect that the path towards better legislation will be easy or short (indeed, its complexity is also indicated by the chapter of this Annual Report specially dedicated to the Office's legislative activities); nevertheless, I am convinced that we are well equipped to this end by the numerous findings made in 2009.

In this respect, I refer not only to practical findings by the Office and those that can be generalized from a professional viewpoint. The year 2009 also undoubtedly confirmed that the general public now has a deeper knowledge of the law. This conclusion is based both on the quality of inquiries made by journalists, which were more detailed and, in a certain sense, more informed, and on the agenda of instigations and complaints, where inquiries were substantially more qualified. However, this was shown and is demonstrable particularly in respect of the requests for consultations. However, the consultancy service placed much higher demands on the professional employees of the Office, in terms of both their time and their expertise. I am naturally glad that the Office is perceived as a truly referential and arbitral institution. On the other hand, I am well aware that its findings are often transformed into an asset for law firms. Consequently, I cannot neglect the issue of the scope of the consultancy which the Office is required to provide under the law, and the related aspect of adequate personnel.

While it is true that the new area of competence entrusted to the Office by Act No. 111/2009 Coll., on basic registers, was accompanied by a certain increase in the number of personnel of the Office, it is currently unclear what requirements will be linked with the tasks following from the mentioned Act in this area. The funds earmarked for the new area of the competence of the Office were also quantified on the basis of estimates of the requirements ensuing from the new agenda, in terms of both technical aspects and personnel. Nevertheless, I consider it a success that we were able to effectively draw money from the European structural funds for this purpose and I am sure that the cooperative spirit of the institution is a cornerstone that will provide a solid foundation for successful performance with our new duties.

I hope that the willingness to cooperate, which is a quality I sincerely admire in the institution over which I preside, will also be reflected on an international level – in organizing the European Privacy and Data Protection Commissioners´ conference in 2010, where commissioners from all over Europe will meet at Prague Castle late in April 2010. It is certainly no minor task to be the organizer of such an important event once every twenty-seven years. However, it is also an honour for the Czech Office to be entrusted by the other EU Member States with organization of the conference. Nevertheless, I shall tackle this challenge with optimism in the spirit of what I sincerely told the employees of the Office at our meeting before Christmas 2009: I am glad that we are a team.

Igor Němec

CONTENS

OFFICE IN NUMBERS – 2009

Inquiries and consultations	inquiries in the Czech Republic	2215
	abroad	111
	consultations	
	for state administration	45
	for local governments	5
	for legal persons	42
	for natural persons operating a business	9
	for natural persons	13
Pleadings and complaints	instigations received pursuant to the Personal Data Protection Act	879
	complaints referred for control	129
Unsolicited commercial communications (competence pursuant to Act No. 480/2004 Coll.)	total instigations	2261
	instigations resolved	1678
	controls initiated	145
	controls completed	131
	administrative decisions on a fine	112
Controls (excluding controls concerning Act No. 480/2004 Coll.)	initiated	143
	completed	131
	referred to other governmental authorities	3
	challenged by objections	38
	objections accepted	5
	objections dismissed	27
	mostly accepted	0
	mostly dismissed	2
Administrative punishment	administrative proceedings for violation of Acts No. 101/2000 Coll. and No. 133/2000 Coll.	89
	misdemeanour proceedings pursuant to Act No. 101/2000 Coll.	10
	misdemeanour proceedings for violation of Act No. 159/2006 Coll., on conflict of interests	1
	appealed decisions on violation of law	43
	appeals dismissed	23
	cancelled and returned for new hearing	7
	cancelled decisions and proceedings discontinued	2
	change in the decision	3
Judicial review	court actions lodged	17
	actions dismissed by the court	5
	decisions cancelled by the court	1
	referred for a decision (pursuant to Article 21 of Act No. 101/2000 Coll.)	3
	court proceedings closed / pending	1/16

Registration	notifications received (pursuant to Article 16 of Act No. 101/2000 Coll.)	3278
	instances of processing registered	2841
	still pending	437
	registrations cancelled	139
	notifications on a change in the processing	817
	proceedings pursuant to Article 17	
	discontinued (no violation)	49
	discontinued for procedural reasons (e.g. notifications withdrawn)	3
	not permitted	1
Authorizations for transfers of personal data abroad	applications for transfer of personal data abroad received (pursuant to Article 27 of Act No. 101/2000 Coll.)	30
	decisions on authorization of transfers	21
	decisions on dismissal	0
	proceedings discontinued for procedural reasons	9
Complaints pursuant to Article 175 of the Code of Administrative Procedure	complaints received	
	complaints found justified	2
	complaints found partly justified	5
	complaints found unjustified	22
Complaints and other instigations related to the procedure of the Office that were not resolved pursuant to Article 175 of the Code of Administrative Procedure	instigations received	0
	instigations found justified	
	instigations found unjustified	
Applications pursuant to Act No. 106/1999 Coll.	applications received	10
	applications resolved	8
	applications rejected	2
Materials published	Journal of the Office (number of volumes)	4
	Bulletin of the Office (number of volumes)	4
Press conferences	regular	2
	extraordinary	1
Legislative drafts on which comments were made	laws	62
	implementing regulations	
	draft Government regulations	11
	draft decrees	101
	other	94
	foreign materials	14

CONTROL ACTIVITIES OF THE OFFICE

In conformity with Article 31 of the Personal Data Protection Act, the Office's control activities are pursued either on the basis of a control plan or based on instigations and complaints. The control plan, whose general part is further described, is drawn up jointly by the President and inspectors of the Office – the document is binding and its fulfilment is regularly evaluated at a meeting of the board of inspectors, which serves as a joint advisory panel for the President and inspectors.

2009 CONTROL PLAN

The Office for Personal Data Protection, based on its experience obtained in control, administrative and registration procedures and in accordance with the interest of society that the Office's control activities be focused, in terms of their planning, on those means of personal data processing that affect the data of a major portion of natural persons, or those situations where the interests of the controllers and processors are concerned with "sensitive groups" of the personal data of society, or that these activities be focused on the new requirements on personal data protection in accordance with the newly applicable legislation, expresses these objectives in the form of the control plan, which was issued for 2009 in accordance with Article 31 of Act No. 101/2000 Coll. by the President of the Office after having discussed the plan with the inspectors of the Office:

I. GENERAL TOPICS FOR SPECIFICATION OF CONTROL ACTIVITIES OF INSPECTORS OF THE OFFICE

1. **Public administration information systems**
2. **Information systems in the area of the 3rd pillar**
3. **Performance of the controllers' duties in connection with authorization pursuant to Article 16 of Act No. 101/2000 Coll.**
4. **Personal data processing in the context of data transfers to third countries**
5. **Personal data protection and non-profit sector**
6. **Other control activities based on the needs and requirements acknowledged by the Office in a certain area**

II. CONTROLS PLANNED AND COMPLETED IN 2009

1. CONTROL OF THE PERFORMANCE OF DUTIES FOLLOWING FROM THE PERSONAL DATA PROTECTION ACT BY A COMPANY WHICH ALSO EMPLOYS FOREIGNERS

The control was concerned with processing of the personal data of both employees and job applicants by a company that employs 3500 personnel, including 2800 nationals of the Czech Republic, 120 agency employees and approx. 30 persons who work on the company's premises, but are employees of different companies.

The inspectors focused particularly on the scope of the data processed within the employees' personal files, on the legal grounds on which the company relied in processing the personal data, on the period for which the data were maintained, and on compliance with the duty to provide information borne by the company as the controller.

The control revealed that, in the personal files of certain employees, the company processed written information on whether or not these employees had been conscripted into the army, although this information was not required for the performance of work within an employment relationship and this processing was at variance with the second sentence of Article 312 (1) of Act No. 262/2006 Coll., the Labour Code, as amended (hereinafter the "Labour Code"), and the personal data was processed within a scope greater than necessary for fulfilment of the given purpose. Similarly, processing personal data on the employees' wives, within the scope of their name, surname and birth number, in the employees' personal files (where the wives were not persons maintained by the employee pursuant to a special regulation) constitutes processing of personal data within a scope greater than necessary for fulfilment of the set purpose. The mentioned personal data processing was at variance with Article 5 (1) (d) of the Personal Data Protection Act, which requires that a company, as the controller, collect personal data only within a scope that is necessary for fulfilment of the set purpose. Where a company processes information on membership of employees in a trade union, it violates the prohibition stipulated in Article 316 (4) (e) of the Labour Code. Since the mentioned information is inadmissible as such pursuant to the cited provision, it also need not be obtained in the sense of the Act and is at variance with Article 5 (1) (d) of the Personal Data Protection Act.

Where the name and surname of a contact person, as well as his telephone number, are being processed in the personal file of an employee whose employment with the company has ceased to exist, this personal data is being maintained for a period of time that is not necessary for the purpose of processing and is thus not in accord with Article 5 (1) (d) of the Personal Data Protection Act.

The company violated Article 5 (2) of the Act when it kept, in the employees' personal files, during employment with the company, documents containing the examination tests and their evaluation drawn up on their recruitment by the company, where the employees consented to the processing of these personal data only for the purposes of the selection procedures.

Where the company recorded information on the employees' nationality in their files, without having their affirmative opinion in this respect, this measure again failed to correspond to any of the other statutory preconditions and constituted processing of sensitive data without the data subject's express consent, which is at variance with Article 9 of the Personal Data Protection Act. Similarly, the company breaches the mentioned provision of the Act when it processes personal data concerning membership in a trade union without having obtained express consent to such processing.

Given the fact that the company, as the controller, fails to advise job applicants or employees of whether the provision of the requested personal data is compulsory or voluntary and in which cases the data subject is obliged to provide personal data for processing pursuant to the special law, as well as of the consequences of refusing to provide personal data to the data controller, it fails to perform the duty pursuant to Chapter II of the Personal Data Protection Act and breaches Article 11 (2) of the Personal Data Protection Act.

In processing the personal data of job applicants and employees, the company (controller) proceeded at variance with the Personal Data Protection Act, because, in the position of the

controller, it collected personal data within a scope greater than necessary for fulfilment of the set purpose; it failed to maintain personal data only for the period of time necessary for the purpose of their proces-sing; and it processed personal data without the consent of the data subjects, while not complying with any of the preconditions for lawful processing of personal data in the absence of the consent of these subjects; and it also processed personal data without fulfilling any of the preconditions under which processing is permitted; and it failed to advise the data subject of whether the provision of the personal data was compulsory or voluntary, and of the consequences of refusing to provide the personal data. A fine was imposed on the company for the demonstrated violation of the Personal Data Protection Act.

2. CONTROL OF PERFORMANCE OF THE CONTROLLER'S DUTIES IN PROCESSING DNA IN THE PRIVATE SECTOR

The control was concerned with a company registered in the Commercial Register whose objects of business included, amongst other things, research and development in the area of natural and forensic sciences and the activities of technical advisors in the area of natural sciences, molecular biology, forensic genetics and good laboratory practice, as well as molecular-biological and forensic-genetic analyses, i.e. genetic analyses drawn up for forensic purposes related to investigations and adducing evidence in criminal matters. In its activities, the company concentrates particularly on science and research, DNA services, publishing activities, consultancy and sale of specialized products for forensic laboratories.

The clients usually order from the company genetic determination of the origin of ancestors, determination of paternity, identification of the senders of anonymous letters, specific certification for sperm or determination of kinship, including determination of the identity of twins. At the present time, the core of the company's activities lies in identification of skeletal remains, including historical finds.

The inspectors focused on compliance with the duties in processing personal data in connection with the submission of biological samples to the company by persons who order DNA analyses. In their orders, the clients also specify the scope in which the samples carrying personal data should be processed. The client's order is documented in the book of contracts, which is one of the basic documentation items used by the company. In respect of each contract performed by the company, the book contains specification of the reference number; the date of delivery of the order (contract) to the company; description of the order; name and surname of the client; specification of the person performing the contract; date of completion of the contract; submission of the contract and the date of payment by the client. The book of contracts also includes specification of notes that characterize the contract in further detail. In accordance with the rules stipulated by the quality guidelines, the records in the book of contracts must be made by hand and may not be drawn up using a computer. The data subject executes the requirement form, whereby he gives his consent to the ordered scope of personal data processing or notifies the company that the given consent to personal data processing has been granted. The company maintains the processed personal data in both printed and electronic form only for the necessary period of time, specifically six months and three weeks. Three weeks are the period of processing of the biological sample pursuant to the given contract for work, while six months constitute the period of time for which the company keeps the biological sample after handover of the work for the reason of possible claims related to defects during the six-month warranty period.

Before each of the above-mentioned cases of processing of genetic samples, the client is provided by the company with a request form, customer information, advance invoice and a sampling set with instructions for use. The latter include particularly "Information for Clients Ordering a DNA Analysis for the Purpose of Testing Paternity, Genetic-Genealogical Examination or Similar Act". By virtue of this information, the data subjects are advised of the management of DNA samples and other personal data in the company. Amongst other things, the data subjects are informed of which personal data the company processes; in what ways this occurs; how the tested samples are labelled; in

what regime the processing takes place, including advice that the DNA samples taken may be processed only with consent of the affected persons; and for what period of time the tested samples will be maintained by the company; and they are also advised that, after expiry of the warranty period, the processed data will be destroyed or that they will be destroyed earlier if requested by the client. Through the mentioned information, the clients are also provided with full advice within the meaning of Articles 12 and 21 of the Personal Data Protection Act. All employees of the company are obliged to maintain confidentiality of facts concerning the activities of the company, including personal data processing. Any unauthorized handling of documents created within the company would be deemed to be gross misconduct. Documents that are sent to the customers must be transformed into the PDF format prior to dispatch. Data in the company's personal computers are backed up, where the usual back-up cycle is one week. With the aim to process only accurate personal data, the company has introduced and maintains, as a preventative measure, a quality assurance system pursuant to the ISO 9001:2000 standard.

The company consistently registers and labels the obtained biological samples during their processing, which fact is already manifested in the actual taking of comparison samples for the DNA analysis, where the client must attach labels to the box containing tampons with the comparison samples in order to prevent unauthorized handling, and must unambiguously mark the box, where the marking is also specified in the "Request for DNA Analysis" form. After completion of the analysis, the oral scrapings (primary samples) sent for expert analysis are returned to the client together with a written counterpart of the expert report. The samples, which are maintained by the company for the necessary period of time, are then destroyed. A record is drawn up of the destruction. Information on the course and results of the analysis are submitted only to the clients or persons who are authorized by the clients in writing to accept the information and results. No subsequent changes may be made in the records of the course of the tests after their termination. Any supplements and changes to erroneously recorded data are performed by crossing out the original data so that it remains legible and specifying the correct data with the initials of the employee who made the correction and the relevant date.

The company processes basic identification details of its customers for the purpose of fulfilling the duty to ensure conclusiveness of the accounting documents. To this end, it has created blank forms of orders with certain prescribed data, which, however, the clients need not specify. These data are maintained for the period stipulated by the applicable legislation. For the purpose of personal data protection, the company also adopts numerous internal rules, which regulate all procedures followed by the employees in processing the clients' personal data.

At the time of commencement of the control, the processing of personal data carried out by the company within its commercial activities had not been notified in writing to the Office.

The control ascertained violation of the Personal Data Protection Act only for the reason that the company, as the controller, processed personal data without having notified the Office of this fact in writing prior to processing the personal data, whereby it failed to comply with Article 16 (1) of the Act; as a result, the Office imposed a fine on the company in administrative proceedings.

3. CONTROL OF PERFORMANCE OF THE DUTIES OF RESPONSIBLE ENTITIES FOLLOWING FROM THE NEW LEGISLATION BASED ON TRANSPOSITION OF INTERNATIONAL DOCUMENTS BINDING ON THE CZECH REPUBLIC

The controls were concerned with the performance of the controllers' duties in processing operational and location data (Act No. 127/2005 Coll.) focused on processing operational and location data from publicly available electronic communications services and public communication networks, including their maintenance for the purposes of investigation, detection and prosecution of serious crime.

Controls were performed, within the deadlines stipulated by the control plan, in four business companies; another control took place subsequently in the fourth quarter of the year. The latter was performed with the aim to ensure sufficient conclusiveness of the control findings. All types of

services where the law requires maintenance of operational and location data, except for mobile telephony services, were thus verified.

All the controls were performed as controls of compliance with all the relevant duties stipulated by the Personal Data Protection Act and Act No. 127/2005 Coll., on electronic communications and on amendment to some related laws, as amended, in processing of personal data pursuant to Article 97 (3) of the Electronic Communications Act.

None of the controls ascertained any breach of the statutory duties. The operational and location data corresponding to the nature of the services provided by the controlled entities are maintained in conformity with the law, i.e. logically separated from other data and for the period stipulated by the Electronic Communications Act, although three of the controlled entities stipulated the period of maintaining the data at the lower limit of the statutory range and two at the upper limit. Furthermore, it was ascertained in respect of four controlled entities that they were being addressed with requests pursuant to Article 97 (3) of the Electronic Communications Act by the Police of the Czech Republic; no such request was ascertained in respect of the fifth entity by the date of termination of the control.

4. PROCESSING OF PERSONAL DATA IN THE SCHENGEN INFORMATION SYSTEM

A governmental control of personal data processing in the Schengen Information System was performed from October 22, 2009 to December 3, 2009. The instigation to include this control in the control plan for 2009 followed from a meeting of the joint supervisory authority (JSA Schengen), which took place in December 2007. The Czech Republic acceded to the Schengen Information System on September 1, 2007 and, therefore, the Office participated in the coordinated inspection.

In accordance with a recommendation of the expert committee for Schengen evaluation of the Member States in the area of personal data protection, a control was also performed at the Ministry of Foreign Affairs in the period from June 30, 2009 to December 16, 2009. The control was concerned with compliance with the duties stipulated by Act No. 101/2000 Coll. in personal data processing related to visa procedures at the embassies of the Czech Republic. The control ascertained violation of the Act.

III. RESULTS OF CONTROLS BASED ON CONTROL PLANS FOR PREVIOUS YEARS THAT WERE COMPLETED IN 2009

1. CONTROL OF PROCESSING THE PERSONAL DATA OF VISITORS TO THE CHAMBER OF DEPUTIES OF THE PARLIAMENT OF THE CZECH REPUBLIC BY THE OFFICE OF THE CHAMBER OF DEPUTIES

This control took place in 2007 and it was concluded that violation had occurred of Article 5 (1) (e) of the Personal Data Protection Act. The Office of the Chamber of Deputies appealed against the conclusions, referring to the exemptions related to the protection of confidential facts. The President acknowledged the objection and referred the case for further investigation. The inspectors continued the control and reached agreement on a change in the regime employed and on introduction of two databases, as the original database was used for various purposes and the period for which the data were maintained thus varied for each of the databases. The control was completed in February 2009 and no violation of the law was noted in its conclusion.

2. PERSONAL DATA PROCESSING WITH THE USE OF VIDEO SURVEILLANCE SYSTEMS

In 2008, the Office also focused its control activities on this area, based on the experience obtained in previous years and also based on increasing pressures for the operation of monitoring systems and introducing them at various levels, often at variance with the interests of individuals in protection of their privacy.

In the period from December 5, 2008 to March 5, 2009, a control was performed at a randomly chosen private company (a major advertising company). The control ascertained that the company kept no database of guests, because employees had to go and meet their own visitors and were responsible for their safety.

3. CONSUMER PROTECTION

Based on a growing interest on the part of both the suppliers and the users in technology allowing for quick and safe identification of data subjects, the Office has noted a society-wide interest in the creation of rules that would limit infringement on the privacy of natural persons to a minimum in relation to the use of chip cards and cards equipped with the RFID technology.

Therefore, in the period from July 16, 2008 to June 2, 2009, the Office undertook a control of a transport company operating in a Central Bohemian city, which uses the technology of customer chip cards.

4. CONTROL OF PROCESSING THE PERSONAL DATA OF THE INHABITANTS OF AN APARTMENT BUILDING

A control of a construction housing cooperative took place in the period from January 10, 2008 to December 4, 2009 The control was concerned with the performance of the duties of the controller, or the processor, in processing the personal data of the members of the cooperative, tenants of apartments, owners of apartments and subtenants. The control was performed also with respect to the amendment to the Personal Data Protection Act, No. 170/2007 Coll., effective from September 1, 2007.

IV. CONTROLS INITIATED IN 2009 BASED ON THE PRESIDENT'S INSTRUCTION

Since 2007, the practice of initiating controls on the basis of a decision of the President has proven useful in serious topical cases. The President of the Office also made similar decisions in 2009.

1. A CONTROL FOCUSED ON THE PERFORMANCE OF THE DUTIES BORNE BY THE STATE INSTITUTE FOR DRUG CONTROL

was carried out on the basis of a serious instigation from the Czech Chamber of Pharmacists to the effect that the duties of the controller, or the processor, pursuant to Act No. 101/2000 Coll. could be breached in activities of the SIDC or in relation to these activities in connection with the operation of the central register of electronic prescriptions and given the fact that an extraordinarily extensive database of sensitive data was being created.

2. CONTROL OF PROCEDURES OF THE MINISTRY OF INTERIOR OF THE CZECH REPUBLIC AND THE MINISTRY OF JUSTICE OF THE CZECH REPUBLIC

On February 5, 2009, the President issued an instruction for initiation of control of personal data processing within the performance of duties pursuant to the Personal Data Protection Act by the Ministry of Interior and the Ministry of Justice in keeping and using the information system of the records of population.

Three controls were promptly performed based on the instruction:
controlled entity: Ministry of the Interior: June 18, 2009 to July 27, 2009;
controlled entity: District Court in Prague 4: March 11, 2009 to June 9, 2009;
controlled entity: Ministry of Justice: August 12, 2009 to October 22, 2009.

No breach of duties in the processing of data on adoption of children was found at the Ministry of Interior. At the Ministry of Justice, breach of the duty pursuant to Article 5 (1) (c) and pursuant to Article 13 (1), (2) and (3) of the Personal Data Protection Act was ascertained in respect of utilization of personal data from the information system of the records of population.

Two administrative proceedings were commenced on the basis of these controls and several others in 2009.

3. CONTROL OF PERSONAL DATA PROCESSING WITHIN THE PERFORMANCE OF THE CONTROLLER'S DUTIES IN RELATION TO THE OPERATION OF A VIDEO SURVEILLANCE SYSTEM pursuant to Act No. 101/2000 Coll., on personal data protection, operated by Prácheňské sanatorium, o. p. s. The control was undertaken on the basis of an instigation from the Ombudsman, Dr Otakar Motejl. The sanatorium specializes in care for clients suffering from Alzheimer's disease. Given the fact that the sanatorium does not keep recordings from the cameras and that the cameras are operated only on-line, this operation is not covered by the Personal Data Protection Act. The control ascertained that the management of the sanatorium was considering the possibility of acquiring and keeping recordings and, therefore, this plan was consulted within the control and the Office pointed out the duties that would arise for the sanatorium in this respect.

4. CONTROL OF COMPLIANCE WITH THE DUTIES OF THE OFFICE OF THE DEPUTY PRIME MINISTER FOR EUROPEAN AFFAIRS in processing the personal data of participants in the EU – U.S.A. summit, which took place on April 5, 2009 in Prague.

The media repeatedly published information on leakage of the personal data of the participants in the EU – U.S.A. summit, which was held in Prague on April 5, 2009. According to certain sources, it was possible to access the personal data of approximately 200 participants in the summit from a publicly available computer at a hotel in Prague. The instigation did not specify any entity responsible for processing the personal data.

First controlled entity: Gestin Holding, a. s.

The control carried out from April 24, 2009 to May 6, 2009 did not ascertain any breach of the duties imposed on the controlled entity by the Personal Data Protection Act; a control of another entity was performed based on the findings obtained in this control.

Second controlled entity: Office of the Government of the Czech Republic

The control performed from May 4 to 26, 2009 ascertained breach of the duties imposed on the Office of the Government by the following provisions: Articles 9, 10 and 13 (1) of the Personal Data Protection Act. The administrative proceedings were not closed by a final decision in 2009.

5. CONTROL OF MEDIASERVIS, S. R. O. related to the performance of the supplier's duties in subscription and delivery of subscribed periodicals. The control was concerned with compliance with the controller's duties connected with processing the personal data of the subscribers and recipients of periodicals.

The company is also active as a processor of the personal data of the subscribers and recipients of periodicals for the controller of these data, i.e. the relevant publisher. The company itself does not use the personal data of the subscribers and recipients of periodicals for marketing purposes, although it could do so given the provisions of Article 5 (5) of the Personal Data Protection Act. The company was only notified of inaccuracies in information provided to the clients within its business terms and conditions. No violation of the laws was ascertained in the control.

6. CONTROL OF GOOGLE CZECH REPUBLIC, aimed at examining the impact of Act No. 101/2000 Coll., on personal data protection, on processing of information collected and further processed in relation to the provision of the Google – Street View service.

Based on an instruction of the President, the control of services provided by Google Czech Republic, s. r. o. was commenced on July 2, 2009, with emphasis on the Google – Street View service.

Controlled entity: August 3 to 5, 2009, Google Czech Republic, s. r. o.

The controlled entity was not found responsible for obtaining video recordings with personal data and, therefore, the competent supervisory authority of the FRG was repeatedly contacted through the foreign affairs department; the findings were then submitted to the German supervisory authority and it was suggested that the latter verify this processing, which fell within the responsibility of an entity established in the territory of the FRG, which had no branch in the Czech Republic.

Based on the complaints of citizens and an application for registration lodged by Google Inc., negotiations were commenced in respect of operation of the Street View service; the negotiations have not yet been completed.

In respect of controls initiated on the basis of the instructions of the President of the Office, it is often not possible to complete a control within a single calendar year and some controls thus continue in subsequent years.

V. CONTROLS INITIATED ON THE BASIS OF AN INSTRUCTION OF THE PRESIDENT IN PREVIOUS YEARS AND COMPLETED IN 2009

In respect of controls initiated on the basis of the instructions of the President of the Office, it is often not possible to complete a control within a single calendar year and some controls thus continue in the subsequent years.

In 2008, this was true of a control performed at the Fund for Children in Need, which was initiated on September 27, 2008 and completed on January 15, 2009 with the conclusion that the practice of the Fund for Children in Need was at variance with the Personal Data Protection Act. Remedial measures were imposed.

FINDINGS OBTAINED BY INSPECTORS IN CONTROL ACTIVITIES

UTILIZATION OF THE RECORDS OF POPULATION WITHIN THE COMPETENCE OF THE MINISTRY OF JUSTICE

The information system of the records of population (hereinafter the "records of population") is related to one of the liveliest cases of personal data processing within the competence and responsibility of public administration and other governmental authorities in the Czech Republic, particularly as a consequence of the legal regulation of the conditions for its utilization by various official authorities. This was one of the reasons why the Office performed control based on two complaints concerning personal data processing within the records of population in 2009. The President of the Office came to the conclusion that it was necessary to check the procedures of the Ministry of Interior and the Ministry of Justice in application of Article 175a of Act No. 6/2002 Coll., on courts and judges, stipulating the conditions for the provision of data from the records of population with respect to the legal framework of the controller's duties pursuant to the Personal Data Protection Act. On this basis, a control team initiated a total of 8 controls concerned with the records of population in 2009, of which six were completed in the same year. Six courts and the Ministry of Justice were subject to the control, where the controls were concerned exclusively with the processing of personal data obtained from the records of population and provision (disclosure) of personal data from this system.

The **controls** began at **District Court I**. The complainant's suspicion was confirmed – it was found that District Court I. had breached the duties stipulated by Article 13 (1), (2) and (4) of the Personal Data Protection Act. Four remedial measures were imposed on District Court I.

In the interest of ensuring objectiveness, **controls were also performed at one regional court, two municipal courts and two district courts**.

All the controls included verification of the relevant duties in personal data processing, as stipulated by the Personal Data Protection Act and Act No. 133/2000 Coll., on records of population and birth numbers and on amendment to some laws, as amended (Act on Records of Population), with application of Act No. 6/2002, on courts, judges, lay judges and on amendment to some other laws (Act on Courts and Judges), as amended, and several other laws.

Audit records kept and provided by the Ministry of Interior pursuant to Article 3 (8) of the Act on the Records of Population were used in the controls. The same procedure was also used for a control at the Ministry of Justice. A total of 96 086 lines of records of access to the records of population were checked, containing information decisive for seeking out a particular inhabitant, identification data on access and the reason and specific purpose of access – i.e. search. A selection of samples was made in those cases where the checked file contained more than 10,000 lines. A total of 470 active user authorizations were checked.

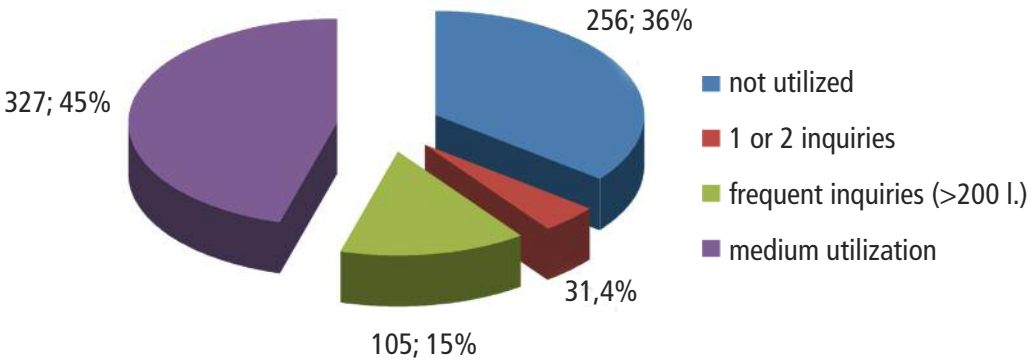
In all these controls, the Office ascertained that the structure of the audit records provided for the purposes of the control did not allow – subject to certain exceptions – for assessment of compliance with the condition stipulated in Article 175a (5) of the Act on Courts and Judges case by case, i.e. that only data required to perform the given task may be used from amongst the data provided in the given case. Furthermore, the Office was forced to state that the means used by the court for processing personal data from the records of population and the manner of their processing did not permit, within the desirable scope, evaluation of the performance of the duties stipulated in Article 5 (3) of the Personal Data Protection Act, i.e. ensuring protection of the private and personal lives of the data subjects in personal data processing pursuant to a special law. Doubts arose in relation to performance of this duty in all cases where the judges or officials sought, as a rule and in all cases, all the available data on the person of interest and his relatives.

Even under these constraints, only the procedure of District Court I. was found to be fully compliant with both the Personal Data Protection Act and the Act on the Records of Population. In respect of all other courts subjected to the control, it was ascertained that they had failed to adopt any specific measures within their competence to effectively prevent unauthorized use of personal data from the records of population – the principles of securing personal data from the records of population were not reflected in the local conditions of the court; the link of the processing concerned to the file created by the courts had not been documented and the conditions stipulated in Article 175a (5) of the Act on Courts and Judges, i.e. that only data required for the performance of the given task may be used from amongst the data provided in the given case, had not been enforced. The courts thus failed to prevent the use of personal data from the records of population beyond the scope of the relevant service task corresponding to the job assignment within the meaning of Article 13 (4) (c) of the Personal Data Protection Act. Thereby they breached the duty pursuant to Article 13 (1) of the Personal Data Protection Act and the duty pursuant to Article 5 (1) (f) of the same Act.

It was also repeatedly found and noted that the courts failed to provide, within automated personal data processing, for the creation of electronic records enabling determination and verification of when, by whom and for what reason the personal data were sought. They also failed to secure proper documentation of the verified cases of processing. As a result, the control of historical cases was very complex and, in some cases, the reason for seeking the data could not be verified. In certain cases, the reason could be inferred only by a repeated identical inquiry to the records of population; however, in some cases, even this procedure did not yield the reason for seeking the data. Only in the case of District Court I. was it ascertained that, with respect to the selected and consistently employed organizational procedure in utilizing the records of population, i.e. particularly that the authorized person usually did not have at his disposal the personal data of the person of interest beyond the scope of the data set out in the Application for an Inquiry to the Central Records of Population, the consequences of the inappropriate structure of audit records created by the Ministry of Interior were minimized at this court.

It was also ascertained that District Court I. did not have available appropriate documentation of the adopted and implemented technical and organizational measures to ensure protection of personal data obtained from the records of population. Similar to Municipal Court I., this court failed to adequately provide for the administration of user authorizations; the sole reason for cancelling such authorization lay in termination of employment. The authorization was maintained as active and valid even several weeks after termination of employment. The same situation was found at District Court II. Authorization was also assigned to persons who did not need to regularly utilize personal data from the records of population. The same state of affairs was ascertained at a further four courts. The assigned authorization was not used by 256 of the total of 719 valid user authorizations; except for one court, where the sample consisted of records for a single month, the records were always checked for two calendar months. Approximately thirty users raised only one or two inquiries during the monitored periods.

UTILIZATION OF THE RECORDS OF POPULATION BY THE COURTS



None of the courts demonstrated that it would deal, in the choice and implementation of the measures to secure personal data from the records of population, with the risks in the sense of Article 13 (3) (c) of the Personal Data Protection Act. The courts failed to utilize the field "reason for inquiry" to achieve the desirable effects of the audit records kept by the Ministry of Interior – they failed to impose, on the authorized persons, the duty to unambiguously and demonstrably link the search with the existing file and, where necessary, create parts of the file corresponding to the purpose (e.g. record in the file). They also failed to use the opportunity to register the use of the records of population in the relevant court application (ISAS and IRES). None of the courts in respect of which violation of the Personal Data Protection Act was noted had performed, by the date of initiation of the control, any check of the use of personal data from the records of population and none of them had specified the methodology for such checks.

The general conclusions were also in no way affected by the finding that, apart from District Court I., whose practice was found to correspond to the requirements for utilization of personal data from the records of population, both pursuant to the Act on the Records of Population and pursuant to the Personal Data Protection Act, users were also found amongst judges and employees of District Court II. and Municipal Court I. whose individual approach complied with all the statutory preconditions stipulated for utilization of the records of population – they performed their searches in relation to the file and within the scope corresponding to the actual needs following from the working task. On the other hand, users were found with respect to whom not a single historical inquiry could be successfully verified.

A majority of authorized users utilized the possibility of seeking data also in respect of relatives of the given persons and, as a rule, they submitted all their inquiries within the widest possible scope. The Office was surprised particularly by search for data on minor children in relation to applications for initiation of distraint proceedings, without there being any indication whatsoever of the need for this. The Office did not find it suitable to include data on children of pre-school age in the file for the purposes of enforcing a claim arising from operation of a public transit system or from a consumer loan in an amount not exceeding CZK 1,500.

Given the scope and form of documenting the use of personal data obtained from the records of population, the control could not ascertain whether any of the controlled judges had breached his duty pursuant to Article 15 (1) of the Personal Data Protection Act, or whether he had proceeded, in processing personal data from the records of population, in a manner other than according to the conditions and within the scope stipulated by the controlled court based on the substantively relevant regulations. The conditions stipulated for the employees of six courts were not strict enough for it to be possible to infer the reasons for the search and the forms and purposes of further use of the sought or verified personal data in the absence of any documents.

Consequently, the Office noted that, in cases where no printouts from the records of population had been made and included in the file, it was not possible to ascertain the state of affairs beyond the fact that the courts had failed to establish local conditions for proper fulfilment of the duty pursuant to Article 5 (1) (f) of the Personal Data Protection Act and Article 8 (2) (b) of the Act on the Records of Population.

The **control at the Ministry of Justice**, which was performed within the same scope as the control at the courts, also led to a conclusion on the breach of duties pursuant to the Personal Data Protection Act. In addition to problems related to the absence of the link to the file or some other appropriate documentation, it was found that personal data had been processed without fulfilling the precondition for admissibility pursuant to the Act on the Records of Population and, in one case, also the precondition of relevance for the case – there was no special legal regulation permitting processing with the use of remote access to data from the records of population for the purposes for which the data were used. The competence of the Ministry, within the general framework of which personal data from the records of population had demonstrably been used, does not authorize the Ministry to utilize the records of population by a self-service dialogue search. The fact that the

Ministry in no way dealt with the consequences of a change in the legal conditions for the use of personal data from the records of population with effect from May 1, 2004, that it failed to propose amendment to the special legal regulations and that it did not adapt the scope of its personal data processing to the applicable laws resulted in a situation where the dialogue search in the records of population repeatedly violated the conditions stipulated in Article 5 (1) (c) of the Personal Data Protection Act.

The Ministry failed to ensure admissibility (legality) of processing in relation to the establishment of individual access rights. The users had been properly advised before their authorization was established; however, the advice did not include a binding instruction to fill-in the field "reason for inquiry" in the inquiry form. The introductory advice also did not entail any instructions concerning the methods of demonstrating the justification of utilization of the records of population. The activities of the Ministry in relation to the employees assigned directly to the Ministry and in relation to the organizational units of the Ministry were limited to establishing user authorizations, securing protection of the infrastructure and monitoring the availability of the application of the records of population for the users in the given sector. The ascertained state of affairs is contrary to the duty of the Ministry, as an entity responsible for the processing, to adopt security measures pursuant to Article 13 (1) and keep records pursuant to par. 4 (c) of the Personal Data Protection Act. Furthermore, it was found that, in processing personal data from the records of population, the Ministry failed to proceed in conformity with the conditions stipulated by the Act on the Records of Population in Articles 8 (2) (a) and (b).

On the other hand, the scope of the data sought in the records of population was always adapted to the working task: no one from the Ministry sought data on the relatives of the given persons and, in a vast majority of cases, the employees sought the address of residence.

The findings from seven courts of various instances and the Ministry of Justice indicate that insufficient attention is paid to the protection of personal data from the records of population. The question whether the District Court I. is just a rare bird or one of the few can be answered only by undertaking individual controls at other courts. The control findings from Municipal Court II., where it was anticipated that the court would respond to the results of the first controls in the given sector, indicate that the former is true.

First three administrative proceedings were commenced in relation to the results of controls completed through a final decision.

HEALTH CARE

A fundamental control performed in 2009 consisted in a **control** performed **in the State Institute for Drug Control** based on instigations sent to the Office by the Board of Pharmacy Owners and the Czech Association of Patients. The control was concerned with compliance with the duties stipulated by the Personal Data Protection Act in relation to commencement of the operation of the central register of electronic prescriptions. The State Institute for Drug Control (the Institute) established the central register of electronic prescriptions on December 31, 2008 as its organizational unit. Trial operation took place during the first quarter of 2009 and, based on the Institute's decision, all pharmacies were to be connected to the central register by March 31, 2009. However, only slightly more than one half of the pharmacies had fulfilled this requirement by the end of 2009.

The central register was established pursuant to the Pharmaceuticals Act with the aim to facilitate prescription of medicinal products by means of electronic prescriptions. The introduction of electronic prescriptions was aimed particularly at preventing prescription fraud involving paper prescriptions, reducing the number of visits by patients to physicians and simplifying the work of both physicians and pharmacists. The Act envisaged that electronic prescriptions would be equivalent to paper prescriptions. The decisive precondition for issuing an electronic prescription was to consist in agreement between the physician and the patient on the form of the prescription, with which the

patient would agree. Given the fact that no physician activated the connection to the central register during 2009, no electronic prescriptions were issued and, consequently, no data generated on the basis of electronic prescriptions of medicinal products were collected. It should be added that, in accordance with the Act, the central register should not contain any data other than those serving for issuing electronic prescriptions.

However, the application of the unused central register was extended based on an ad hoc decision of the Office. As a result, data on patients copied from paper prescriptions and also data on patients to whom medicinal products subject to limitation have been sold were stored in the central register.

The control thus concentrated on the legality of collection of the personal data of patients that were sent to the Institute by pharmacies in the form of reports, both on medicinal products dispensed on the basis of a paper prescription and on dispensed medicinal products subject to limitation.

The Pharmaceuticals Act requires that pharmacies and pharmacists keep records of dispensing medicinal products with the use of their codes and that they maintain these records for a period of 5 years. Furthermore, pharmacies and pharmacists are obliged to provide the Institute with information on dispensed medicinal products. The duty to maintain information on medicinal products dispensed on the basis of a paper prescription was already borne by the pharmacies pursuant to the previous legislation. According to the Act on Care for Health of Population, the Institute is authorized to perform supervisory control activities and, in this relation, it is authorized to become acquainted with the patients' personal data. The amendment to the Pharmaceuticals Act neither restricted nor extended this authorization of the Institute. Thus, the Institute was not entrusted with the authority to collect personal data; it only obtained the right to gather information on the dispensed medicinal products. The decision of the Institute thus exceeded its competence under the law. The inspector performing the control rejected the argument put forth by the Institute that, through the decision to collect information on all issued prescriptions, including the personal data of the patient, physician and pharmacist, the Institute fulfilled the requirement that each medicinal product can be traced and found within the entire chain from its manufacture to the final consumer. This is also ruled out by the relevant EU Directive, 2001/83/EC, which stipulates that the paths of the individual medicinal products need to be monitored only in the phase of distribution, but not during dispensing to the public.

Within the performed control, it was also necessary to deal with further requirements for keeping records of medicinal products, such as the requirement for fulfilment of the Institute's duty to ensure provision of information collected within the system of pharmacovigilance to other Member States within the European Medicines Agency, in conformity with the instructions of the Commission and the Agency, or fulfilment of the duty to provide an overview of dispensed medicinal products to meet the requirement to respond, operatively, effectively and appropriately, in the national environment, to measures adopted by the European Commission, the European Medicines Agency and other bodies of the European Union and the WHO (the World Health Organisation). This includes particularly those cases where the Institute would withdraw medicinal products from the Czech market based on a decision of the mentioned bodies and organizations. The control concluded that the Institute's competence in this area did not include the statutory authorization to process the personal data of patients, physicians and pharmacists. The inspector entirely rejected the arguments of the controlled entity that the Institute was obliged to collect personal data in relation to keeping records of medicinal products dispensed on the basis of a paper prescription within fulfilment of tasks in the area of prices and payments for medicinal products.

The inspector performing the control thus stated in the control protocol that the Office had no statutory duty to collect the personal data or sensitive data of patients in the central register or elsewhere in the form of reports on medicinal products dispensed on the basis of a paper prescription. Consequently, when requiring the pharmacies to provide personal data and sensitive data to the central register, the Institute acted beyond the scope of the Act. The Institute imposed this duty on pharmacies and pharmacists within its information material – the Journal – in spite of the fact that,

pursuant to Article 9 (c) of the Personal Data Protection Act, sensitive data may be processed only on the basis of a special law. However, a decision of the Institute cannot replace a law and the will of the legislators expressed in the law. Indeed, the Institute had not been authorized to collect health-care data on almost all the citizens of the Czech Republic by any law.

Furthermore, the control was concerned with collection and processing of personal data in connection with dispensing medicinal products subject to limitation without a medical prescription. These include medicinal products containing pseudoephedrine, which are abused for the manufacture of illegal drugs. The control concentrated on justification of the communication between the pharmacy, i.e. the pharmacist, and the central register, where it is first determined whether the given customer has already received a medicinal product subject to limitation from any pharmacy and in what quantity. In the second phase, the pharmacy sends a report to the central register containing data on the medicinal products just dispensed; it can further browse, change or cancel the record related to this information. The Institute decided on including a medicinal product in the group of medicinal products subject to limitation that are dispensed without a medical prescription through an administrative decision whereby it imposed on the pharmacies and pharmacists the duty to check, in dispensing medicinal products subject to limitation, by means of remote electronic access to the central register, whether such products have already been dispensed, either based on the number of the person insured (birth number) or on identification personal data of the patient, including a request for presenting an insurance card or identity card.

The competence of the Institute to issue decisions in the area of medicinal products is derived from the Pharmaceuticals Act. Based on the statutory authorization, the Ministry of Health stipulated, in Decree No. 228/2008 Coll., on registration of medicinal products, that, in respect of an application for including a product among medicinal products subject to limitation dispensed without a medical prescription, it is necessary to furnish justification of the proposed manner of dispensing and a proposal for limiting measures (e.g. age control, limitation of the number of dispensed packages, recommendation from a pharmacist, records of persons, records of the dispensed packages). The duties of pharmacies and pharmacists in dispensing medicinal products subject to limitation without a medical prescription are stipulated and specified by Decree of the Ministry of Health No. 378/2007 Coll. The Decree requires that, rather than the Institute, the pharmacists, when dispensing a medicinal product subject to limitation without a medical prescription, verify that the conditions for limitation of dispensing stipulated in the decision on marketing authorization are met, check the identity of the person requesting the medicinal product and provide this person with the information necessary for safe use of the medicinal product. Furthermore, the Decree requires that pharmacies keep records of dispensing these products within the scope of the name, surname, insurance number of the insured person or date of birth and brief record of the state of health of the person to whom the product was dispensed, including a record of an interview which should take place to an extent essential for evaluation of the indication.

It follows from the above that no legal regulation enables the Institute to require from pharmacies, and subsequently collect and further process, the personal data of persons, that the pharmacies keep in the records of dispensing of medicinal products subject to limitation without a medical prescription. The duty to process and maintain personal data is borne, pursuant to the law, exclusively by the pharmacies, not by the Institute.

When collecting data from pharmacies, the Institute was in the position of a personal data controller. When sending data to the Institute, the pharmacies were in the position of a data processor for the Institute.

The control ascertained that the Institute failed to secure protection of the data sent by the pharmacies so as to prevent access to the data by unauthorized persons, also other than pharmacists. The Institute also failed to draw up and document appropriate technical and organizational measures to protect these data. The Institute entirely neglected any supervision of the pharmacies as data processors and their control.

Based on all the findings, the inspector performing the control concluded that the Office had breached the duties of a personal data controller and imposed remedial measures to eliminate the ascertained shortcomings. The measures imposed were based on the duty of the Institute not to collect the personal and sensitive data of persons in the central records by means of reports on dispensing medicinal products on the basis of a paper prescription and, furthermore, by means of reports on dispensing medicinal products subject to limitation without a medical prescription. Moreover, the inspector imposed on the Office the duty to destroy personal and sensitive data that had been collected in this way.

The Institute lodged a proper appeal against the control finding. In its appeal, it strictly rejected the conclusions set out in the control protocol. In the second-instance proceedings, the President of the Office dismissed the objections of the controlled entity against the control protocol and fully upheld the conclusions drawn by the inspector performing the control, including the relevant arguments. The President stated that no legal regulation authorized the controlled entity to process personal data in the central register in the relevant manner. A further decision of the President was rendered in this case, where the President dealt with an objection against the imposed measure to destroy the data. The imposed measure required that the Institute destroy personal data kept in the central register without statutory grounds. The President dismissed the objection and stated, in his second-instance decision, that the control findings indicated that the collected personal data were kept unlawfully, and thus confirmed the control protocol to the full extent.

On the basis of the final decision of the President of the Office, the Director of the Institute sent a message to the inspector performing the control to the effect that he would accept all the imposed remedial measures and that they would be complied with within the set deadline.

Based on the final decision, the Office initiated administrative proceedings against the State Institute for Drug Control on the grounds of a suspected administrative offence. The proceedings had not been completed by the end of 2009.

The results of this control, which was extensively covered by the media, clearly documented that the State Institute for Drug Control exceeded its competence and, within its activities, which were tolerated by the Ministry of Health, neglected the rights of the patients to protection of data and their right to privacy. The need to protect privacy remains, whatever the trends may be, a fundamental task, not only for data protection officers, but also for those who care about fundamental rights and freedoms. If concerns related to protection of data and privacy are not taken into consideration, a real danger of undermining the most fundamental human rights and freedoms can arise. In this respect, it cannot be successfully argued, for example, that it is necessary to ensure protection against persons who abuse pharmaceuticals to manufacture illegal drugs. It is absolutely clear that there must be a different way of preventing drug addicts from abusing medicaments than unlawfully processing personal and sensitive data on a majority of the citizens of the Czech Republic.

In the area of protection of personal data and privacy in health care, the Office also dealt with a number of instigations, both when **replying to inquiries and requests and when providing consultancy**. A vast majority of inquiries and consultations in the area of health care are concerned with keeping medical documentation, i.e. application of Act No. 20/1966 Coll., on care for health of the population, and the implementing regulations. Increasingly often, the Office is addressed by patients who were not allowed to inspect their medical documentation or who suspect that their medical documentation has been perused by an unauthorized person, or who claim that their medical documentation be submitted to a new examining doctor. In a certain way, the Office substitutes for the activities of the competent supervisory authorities.

A number of inquiries and requests for assistance are concerned, in their nature, with the conduct of health-care facilities, and the Office must refer the inquiries to other institutions.

Based on the received instigations, in 2009, the inspectors of the Office carried out over 15 investigations in health-care facilities and institutions whose activities are directly related to health care.

On the basis of a complaint, an inspector of the Office undertook **investigation in a health insurance company** which, according to the complainant, required exclusively cashless transfers for payment of funds in relation to the use of preventative programs by the insured person. It thus requested bank details from persons insured by the company, since it intended to pay funds only into the insured person's bank account. This decision was adopted on the basis of previous negative experience when contributions were abused by unauthorized persons. However, during the investigation, it was ascertained that, in cases where the insured person insisted on not providing his bank details and requested that the payment be made in cash, the request was satisfied. The problem lay in the fact that the insurance company failed to provide information on this option in advance and, in some cases, even the employees of the insurance company failed to provide the correct information. At the same time, it was ascertained that, in this relation, the insurance company had been collecting, from its patients, information on the name, surname, mailing address, account number and date of issue of the account statement. Thus, beyond the scope of its authorization to process personal data, it processed personal data within the scope of the bank account number and the date of issue of the account statement; however, it did so with the consent of the patient. Furthermore, it was found that the health insurance company was utilizing information on the mailing address to check the place of residence of the insured persons in its database. This reason lay in the fact that the vast majority of insured persons failed to comply with their statutory duty to notify the health insurance company of a change in their place of residence. **The inspector of the Office did not find this procedure to be at variance with the law.**

Based on an instigation, the inspector performed a control in a teaching hospital. General practitioners had left this hospital without any replacement being found. Given the fact that the hospital was unable to secure health care for approx. 5,000 patients, it decided to transfer these patients to the care of some other non-governmental health-care facility, which had agreed with this. Therefore, the hospital sent the patients a letter in which it informed them that it was unable to provide health care by general practitioners and, for this reason, it was **transferring** their **medical documentation to another** non-governmental **health-care facility**. Furthermore, in the letter, it invited the patients to express their potential disagreement with this transfer to another physician with whom they would be registered. The letter was printed by the hospital on the letterhead paper of the new non-governmental health-care facility. Together with this letter, the envelope also contained an advertising leaflet, offering the services of the non-governmental health-care facility. As a result of the fact that the letter was printed on the letterhead paper of the new non-governmental health-care facility, the patients justifiably believed that they had already been registered and their medical documentation transferred.

In response to complaints from a number of patients and on the basis of an intervention by an inspector of the Office, the hospital immediately terminated the entire process of transferring the patients.

On the basis of a complaint by the mother of a minor patient, the inspector of the Office performed a control at a paediatrician. The mother of the minor patient advised the doctor that she had chosen a new examining doctor and asked for the medical documentation of her daughter.

The doctor used a courier service to **hand over the medical documentation to the new examining doctor**. It happened that the consignment was not delivered to the new examining doctor. In spite of the efforts of the doctor, who had contacted all the physicians in the city and its vicinity, the medical documentation of the minor patient was not found. The doctor thus breached her statutory duty to adopt measures to prevent unjustified loss of personal data.

The same approach to the sensitive data of patients was ascertained in respect of two specialist doctors in Prague. Both physicians, operators of a non-governmental health-care facility, alternately used common premises for their activity. Based on an instigation, it was found that medical documentation kept by the two doctors was placed in unlocked filing cabinets located in the waiting

room in front of the surgery. During the inspection, it was found that the unlocked and, in some cases, slightly open filing cabinets, containing over 600 medical documentations of the patients of the two doctors, were accessible to all the visitors in the waiting room. Both doctors thus violated the provisions of the Personal Data Protection Act. On the basis of the inspector's finding, a fine of CZK 50,000 was imposed on each of the doctors. However, the decisions have not yet come into legal force.

During the year 2009, the Office received a number of complaints about the **security of the medical documentation** kept by major health-care facilities, particularly hospitals, in electronic form. The subject of the complaints lay in the fact that, in the health-care facilities, the doctors and medical personnel have unlimited access to medical documentation also in those cases where no health care is being provided to the given patients.

On the basis of the controls performed in the area of the security of personal and sensitive data constituting the contents of medical documentation, it can be summarized that the approach by the doctors and supervisory health-care authorities still tends to be based on customs and does not reflect the principles of the right to protection of the patients' data.

SCHOOLS

The controls again revealed a historical problem related to the scope of personal data requested in acceptance procedures. Given the fact that, at the present time, acceptance of children into pre-school facilities falls fully within the competence of the given kindergartens or nurseries, the scope of the processed personal data is based only on the acceptance criteria that are established by the given facility with respect to the specific circumstances (not enough vacancies and too many applicants or vice versa): the place of residence, employment of the mother, age and, in some cases, number of siblings. Furthermore, it is necessary to process contact details for the purpose of potential communication with the parents. All other personal data are redundant. If a child is not accepted by the facility, these data may be maintained only up to the age of six, when the child reaches school age, should the kindergarten believe that the parents will again apply for acceptance to the same kindergarten. In other cases, the personal data should be destroyed without delay.

The controls also revealed another old issue: There are several institutions that may require processed personal data from all governmental and private institutions, such as the Police of the Czech Republic, the National Security Authority, the Security Information Service, as well as the tax authorities and the Department for Social and Legal Protection of Children. Therefore, where a school processes personal data (even without authorization, after expiry of the necessary period of their processing), it must submit them to these institutions, even though the data may be obsolete and thus incorrect.

Pedagogical-psychological consultancy centres (hereinafter "consultancy centres") aim to assist parents with resolving their children's problems. The consultancy centres are also required to cooperate with schools and kindergartens, because applications for postponing the beginning of school attendance or applications for special treatment in case of any disability often require assessment by a consultancy centre.

From the viewpoint of the Family Act, where the main responsibility for bringing up children is entrusted to the parents, it is entirely ruled out that the school communicate with a consultancy centre without the knowledge and consent of the parents.

The Office received a complaint that a teacher in a kindergarten refused to submit the filled-in questionnaire of a consultancy centre to the parents. Within the control, the inspector reached the following legal opinion: If the parents ask for assistance from a consultancy centre, the consultancy centre may in turn request assistance from the given elementary school or kindergarten and request that the latter fill in a questionnaire concerning the behaviour of the child in this facility. The teachers are not obliged to fill in the questionnaire (this is not part of their working duties); if they voluntarily do so, the consultancy centre becomes the controller of the personal data (often very sensitive)

contained in them. Its employees work with these data with the responsibility and duty to maintain confidentiality based on their occupation. If the parents want to know the contents of the questionnaire, they may ask the consultancy centre for information about the personal data which it processes and they also have the authorization pursuant to Articles 12 and 21 of the Personal Data Protection Act.

Therefore, the teacher sends the filled-in questionnaire to the consultancy centre with the consent of the parents (as only with their consent will the child be examined in the consultancy centre); however, he is not obliged to advise them of its contents.

In the controls, the inspectors again encountered the issue related to the annual reports of schools. Schools process the personal data of their employees including sensitive data on their absence or possible termination of employment as a consequence of deterioration of their state of health, as well as disability pensions, within the performance of the employer's duties. However, pursuant to Article 13 of the Personal Data Protection Act, they must prevent access to these data by an unauthorized person. Processing for some other purpose is possible only on the basis of a statutory authorization, which is embodied in the Schools Act and Decree No. 15/2005 Coll., stipulating the rules for publishing reports on schools. Article 7 is concerned with the personal data of teachers: "The annual report on activities of the school shall always include: [...] c) a general description of the school's personnel, [...] g) information on ongoing education of pedagogical workers [...]." The duty stipulated by the Decree is fulfilled by specifying the name and surname of the individual employees of the school and, if appropriate, their professional attributes. No other personal data, specifically, e.g., data on their state of health and the reasons for long-term incapacity to work, may be published.

PERSONAL DATA PROCESSING IN CASTING

In 2009, within its control activities, the Office dealt with the performance of the duties of the controller and processor in processing the personal data of natural persons who registered for casting for a reality show.

1. The purpose of processing the personal data of natural persons who have registered for casting for a particular reality show is determined by the entity that announced the casting for the given reality show, who is thus in the position of the personal data controller. However, in some cases, this entity does not process the personal data of the natural persons who have registered for casting for a given reality show itself, but rather entrusts the processing to other entities, with which the controller has concluded the relevant agreements to provide, not only for casting for the given reality show, but also for the creation or production of a TV program for the reality show, for the presentation of the reality show and also, subsequently, for the provision of information to interested parties on the development and course of the given reality show on the website, where these entities are in a legal relationship with the controller (processor). Since these further entities also determine the purpose and means of personal data processing and are responsible for the processing, they are also controllers. Given the fact that none of the grounds for waiver of the notification duty stipulated in the Act covers this processing, the controller has a notification duty towards the Office.

The control ascertained violations of the Personal Data Protection Act:

- the duty to inform the data subject, upon granting of his consent, of the purpose of the processing and of the personal data for which the consent is being granted, to which controller and for what period the consent is being granted, and also that the controller must be able to demonstrate the consent of the data subject to the personal data processing throughout the term of the processing;
- to inform the data subject of the scope in which and the purpose for which the personal data will be processed, who will process the personal data and in what manner and to whom the personal data may be disclosed, unless the data subject is already acquainted with this information, and that the controller must inform the data subject of his right of access to the personal data, the right to have his personal data rectified, and other rights stipulated in Article 21 of the Act.

As a consequence of these ascertained violations of the Personal Data Protection Act, the corresponding remedial measures were imposed on the controlled entity and deadlines were specified for their performance within the control protocol.

However, consent granted by minors constitutes a serious issue: Article 8 of the Civil Code stipulates: **The capacity of a natural person to acquire rights and assume obligations through his or her own legal acts (legal capacity) shall arise to the full extent upon reaching legal age**. Article 9 further specifies: *Minors shall have capacity only to those acts that are, in their nature, appropriate to the intellectual and volitional maturity corresponding to their age*. On the contrary, the parents are responsible for the *emotional, intellectual and moral development* of minor children (cf. Article 31 of the Family Act and Articles 217 and 217a of the Criminal Code). In the specific case of the controlled casting agency, the formulation *"business activity of the agency"* was so indefinite that it was not clear to what the client actually gave his consent and, therefore, we requested the consent of the statutory representatives for all minors.

VIDEO SURVEILLANCE SYSTEMS

The Office has traditionally paid major attention to the area of personal data processing with the use of video surveillance systems with recording equipment. The consistency in the Office's approach to this aspect has also been reflected in the increasing number of inquiries, both within the preparation of registration of these systems and generally from citizens and various companies and institutions. For example, the department providing consultancy received over 250 written complaints and inquiries related to video surveillance systems in 2009. Over 30 complaints were forwarded for control.

The quality of the **applications for registration** in the public register **lodged by the administrators of the video surveillance systems** has also improved. Nevertheless, there are still many administrators with whom the Office held consultations already during the registration proceedings. The following could be considered to be typical examples of registration notifications.

In the following case, the data controller, specifically a relatively small town, notified the Office of its intention to **process the personal data** of its **customers** (diners) and third parties through 16 stationary cameras that would monitor catering premises, the area for placing dirty dishes and cutlery, the hall and the adjacent entrance area owned by the party to the proceedings. The notifier stated that the video surveillance system would serve as an aid in resolving cases of damage to the property of the controller and the customers (diners), that the recording would be used to identify cases of vandalism, misconduct and theft, which had been repeatedly occurring in respect of both the property of the party to the proceedings and the property of the diners (broken doors, bicycles stolen in front of the building, a jacket stolen from a hanger, cut table cloths, stolen cutlery, etc.). The personal data would be processed without the consent of the data subjects and the recordings would be maintained for a period of 3 months. Given the justified suspicion of unauthorized personal data processing, proceedings were commenced against the party ex officio. In the subsequent proceedings, the Office did not permit the processing of personal data within this scope.

In another case, the party to the proceedings notified the Office of its intention to **process the personal data of the members of a city assembly, employees** and third persons **during meetings of the city assembly** by means of a single stationary camera with sound recording equipment located in the meeting room of the city authority, for the purpose of drawing up and subsequent control of the minutes of the meetings of the city assembly, where the recordings would be maintained for a period of 30 days.

Based on the aforementioned facts, there was a justified concern that the personal data processing could result in violation of the Personal Data Protection Act and, for this reason, the Office initiated proceedings ex officio in accordance with its statutory duty. Again, in these proceedings, the Office did not permit the operation of the video surveillance system within the proposed scope.

In another typical notification, the party to the proceedings (operator of a restaurant and bar) notified the Office of its intention to **process the personal data** of its **customers and employees** in one of the largest clubs in Prague, consisting of a luxury restaurant and a club with a dance floor, seating premises and bars, without the consent of the data subjects, by means of 60 stationary and mobile cameras monitoring the premises of the cub (entrances, bars, restaurants and corridors) in that the monitoring would be focused on the premises of the luxury restaurant where the cash of the customers was handled, specifically the bars and cash registers, for the purpose of controlling these transactions. In the area of the club with the dance floor, seating premises and bars, the monitoring would cover practically the entire area for the purpose of protecting the property and rights of the customers, the notifier and the landlord against persons intending to take advantage of the inadequately illuminated area to commit crime. Again, the Office commenced administrative proceedings ex officio. Within the proceedings, the party itself decided to make a change in the use of the video surveillance system.

In relation to the provision of consultations related to the operation of video surveillance systems, the Office most frequently encounters inquiries made by employees in respect of **monitoring** their **workplace** by the employer. In spite of the fact that the operation of video surveillance systems without recording equipment, i.e. in the on-line regime, does not fall within the Office's jurisdiction, in view of the fact that such conduct can be at variance with both the Charter of Fundamental Rights and Freedoms and the Civil Code, the complainants are advised as to how they should proceed in these cases. Most often, the complaints relate to misuse of a video surveillance system to impose disciplinary sanctions. In these cases, the cameras are set in such a manner that the processing does not attain the declared purpose – protection of property. Where the pleadings are specific, the Office refers them to the locally competent district labour inspectorates. However, most pleadings do not contain the address of the entity against which they are aimed. Therefore, we recommend that the complainants turn to the competent labour inspectorates.

At the same time, within its supervisory competence, the Office cooperates with the State Labour Inspectorate and the individual district labour inspectorates. Where the labour inspectorates themselves reach the conclusion that the given case also entails a suspicion of violation of the Personal Data Protection Act, they refer the relevant part of the pleading to the Office.

A number of requests for information are related to the use of **municipal video surveillance systems**. The reasons for their establishment lie particularly in efforts by the local government to secure public policy. Frequently, citizens inquire about the fact that a municipality operates a video surveillance system that covers their house, property or garden with a swimming pool. However, most frequently they complain about cameras directed at the windows of a private home. In 2009, the Office also received a request for assistance from opposition politicians who were concerned that they were being continuously monitored by a video surveillance system.

Within their supervisory activities, the inspectors of the Office undertook some 30 incidental controls concerned with personal data processing by means of a video surveillance system. For example, based on an instigation from the President of the Office, a control was performed in a statutory city whose municipal police, as the operator of a video surveillance system, had provided a recording to a private nationwide television channel. The recording contained the personal data of persons recorded at the place of disbursement of social support benefits. This recording was repeatedly published in television news. The city, and specifically its municipal police force, also placed cameras in the inner premises of the city hall and unlawfully disclosed the recordings, including images of specific persons, whereby it committed an administrative offence. The inspector of the Office made a decision on imposing a fine.

Further controls concerning the operation of a video surveillance system included a control performed in another statutory city. The city installed a video surveillance system in an accommodation facility serving for both permanent and temporary accommodation of its citizens to whom the city was obliged to provide a substitute residence in the form of substitute accommodation or shelter. The

cameras were operated by the municipal police. It was ascertained and documented that the cameras monitored the area around the accommodation facility, the entrance to the facility and all the corridors in a several-storey building. A permanent house service was available in the facility. The reason lay in the fact that problems were constantly occurring in the building of the accommodation facility and the city was unable to permanently deploy a police officer in the building. Therefore, the video surveillance system was intended for continuous surveillance aimed at eliminating disruption of public order and violation of the house rules, to prevent unauthorized use of electricity, non-compliance with hygiene standards in waste management and destruction of the common premises of the building, as well as to check that the residents did not allow unauthorized persons to enter the building. While the city dealt with the aspects of personal data protection within the preparation of the video surveillance system, it resolved that, from the viewpoint of the right of the personal data controller to protection of its rights and legally protected interests, it was allowed to monitor the citizens. The city did not request any consent from the residents and did not respond to their protests. In addition to visibly installed cameras and a sign which only stated that the building was safeguarded by a video surveillance system, the residents were provided with no information whatsoever, particularly that the cameras were operated and recordings made by the Municipal Police.

In his finding, the inspector concluded that the city violated the Personal Data Protection Act. The right to privacy in an accommodation facility is guaranteed by Art. 7 (1) and Art. 10 (2) of the Charter of Fundamental Rights and Freedoms. The affected persons also have the right to protection against unauthorized collection of personal data on them and their families. Guidance for assessment of whether interference with privacy, such as the collection of camera recordings, can be tolerated in view of the declared purpose, i.e. prevention of undesirable phenomena, can also be found in court case-law. For example, the Constitutional Court of the Czech Republic stated, in its Award ÚS 191/05, that a fundamental right or freedom may be restricted only in the interest of another fundamental right or freedom. When considering the priority of one of the two colliding rights, it must be evaluated whether all the options to minimize the interference with the fundamental rights of another person have been utilized. In its decision, the city preferred its interest consisting in protection against minor thefts and misuse of the premises to the right to protection of privacy and personal life. Also with respect to the ruling of the Constitutional Court, it is clear that the city's approach was wrong.

Another control was performed on the basis of a complaint that the municipal police allegedly posted photographs taken by the municipal video surveillance system on their website. In the photographs, it was possible to recognize only the figures of the persons present in the monitored area. Within the control, the inspector ascertained that pictures obtained by the municipal cameras were indeed published and made available on the website of the municipal police. The recordings depicted a parade of veteran cars in the municipality. On their website, the municipal police made available selected and modified pictures obtained by the video surveillance system of the municipality established for the purposes stipulated by the Municipal Police Act, as well as selected pictures from social events. Before the photographs were made available to the public on the Internet, the faces of persons were blurred. As a result, individuals could not be recognized and directly or indirectly identified – they were thus rendered anonymous. This was true particularly of pictures taken within control of passage through intersections. Consequently, no personal data within the meaning of the Personal Data Protection Act were involved.

The above-described controls have in common that they related to the use of video surveillance systems with recording equipment by municipalities, towns and cities through the municipal police forces which they had established. Pursuant to the relevant law, municipal police perform the tasks specified by the founder. According to the Municipalities Act, municipalities, towns and cities are obliged to secure public policy on public premises. The inner premises of buildings owned by a city or the inner premises of a city hall are not public premises. Within the supervisory activities, the Office

ascertained, for example, that the municipal police of a city in western Bohemia was instructed by the mayor to monitor, on their displays, recordings obtained from cameras installed on residential buildings owned by the city. The municipal police thus utilize video surveillance systems that are acquired with the use of the public funds of the city or State to monitor their own citizens, but unfortunately without any internal or external control. Personal data processing by the municipal police aims to secure public policy. It is thus unacceptable that the acquired recordings be used in any other way than to document detected criminal offences or misdemeanours.

Inspectors of the Office performed a number of controls in **residential buildings**. These residential buildings were owned by natural persons, municipalities or cooperatives. A common feature of all these controls lay in a complaint raised by one of the tenants in respect of the operation of a video surveillance system without consent of the residents, mostly augmented by the fact that the operator of the video surveillance system failed to respond to disagreement of the residents with the monitoring. The Office has been dealing with the issue of video surveillance systems in residential buildings in the long term. It published its statement on this subject in May 2008.

The inspectors also encounter the fact that video surveillance systems were installed on the basis of a recommendation from the local police, both municipal police and the Police of the Czech Republic. The principal issue connected with video surveillance systems in residential buildings lies in the fact that they are primarily intended and used for monitoring persons, rather than for the protection of property, as originally declared. Only in a negligible number of cases are the recordings actually submitted to the competent authorities with the aim of enforcing penalties. The use of video surveillance systems in cooperative buildings or buildings owned by associations of owners is a separate issue. This entails a conflict of the right to make common decisions with the right of an individual to express his agreement or disagreement with the processing of his personal data. The decision made by the board of the residential building to install a video surveillance system, which is submitted for approval to the meeting of the residents, usually prevails. The fact that a majority has prevailed over disagreeing persons is then presented as the consent of all the owners or users of apartments. However, this incorrect conclusion is at variance with the right of everyone to state his own free consent to the processing of personal data. **In all the controlled cases, it was concluded that the operation of the video surveillance system was at variance with the law, as the protected interest did not prevail over the right to protection of privacy. The value of protection of privacy connected with residence is much greater than the value of identifying the person who has stolen, e.g. a doormat. It can be further summarized that video surveillance systems in residential buildings are mostly unable to fulfil the declared purpose and that the acquired recording does not provide the most suitable means of securing order in the building. Based on the performed controls, fines in the average amount of CZK 50,000.00 were then imposed in the subsequent administrative proceedings on an administrative offence.**

Several complaints were submitted to the Office in 2009 as a result of **operation of video surveillance systems in swimming pools and water parks**. It was ascertained that the operators of these facilities often installed cameras throughout their premises. The specified purpose most often consisted in protection against theft. In two cases, it was determined that cameras were installed only in the women's changing rooms and showers, with justification that things had been stolen only from lockers in the women's changing rooms. In one case, the operator of the swimming pool published a photograph of a person suspected of theft on the premises of the facility, both on his website and in the entrance premises. However, the recording with the alleged theft was not submitted to the police.

During the control, it was ascertained that over 120 cameras were installed throughout the premises. The visitors were absolutely inadequately informed of who could view the recordings, to whom they could be submitted, etc. **Such conduct is at variance with the Personal Data Protection Act**. The individual controls performed by the inspectors in the area of video surveillance systems with

recording equipment were also concerned, e.g., with installation of cameras in the corridor in front of the changing cabins of a **sports facility**.

Based on relevant complaints, several controls were performed in respect of **video surveillance systems in schools**. These were often complaints made by teachers who were concerned that they were unlawfully controlled by the headmaster. Given the fact that recordings obtained from the cameras could be maintained only in those cases where the cameras were used to protect the property of the school or children (other reasons, such as combating bullying or protection of children's health, were found to be irrelevant and recordings ineffective), the schools came to the conclusion that they needed to keep recordings only from cameras installed in cloakrooms and, as appropriate, corridors, optimally after school hours and during holidays. However, surprisingly, all the controlled schools eventually concluded that they did not require the camera recordings.

In 2009, the Municipal Court in Prague ruled on an action lodged by an elementary artistic school against the Control Protocol and Decision of the Office on imposing a fine of CZK 90,000, related to unauthorized processing of personal data by means of a video surveillance system with recording equipment. The Municipal Court dismissed the action and agreed with the conclusions of the Office, according to which the school, as the operator of a video surveillance system with recording equipment acquired and processed the personal data of teachers, students and other persons at variance with the Personal Data Protection Act and interfered with the privacy of the affected persons. The school management used the video surveillance system to monitor compliance with the teachers' working duties. In its decision on installation of the video surveillance system, it failed to use other, less invasive means of preventing potential negative phenomena.

In several cases, the inspectors performed control at entities that had installed only imitation cameras on their buildings for preventative reasons. In this case, the duties stipulated by the Personal Data Protection Act are not applicable, as personal data are not actually collected.

Controls were also performed in **a psychiatric clinic, a sanatorium for senior citizens, an old people's home and a district hospital**. In these facilities, the video surveillance systems were used by the responsible personnel to ensure that they have instantaneous information on the whereabouts and behaviour of the clients. The nature of the system thus lay in its on-line use. Nevertheless, everything was recorded in all these facilities. In the opinion of the Office, this was redundant in all these cases, as the recordings could no longer serve for the provision of immediate assistance to the clients.

A control took place in a building that housed a foreign **embassy** and also **a company operating a hotel**, where the latter monitored the entire building through a video surveillance system with recording equipment. After intervention by an inspector, the regime was changed so as to maintain privacy not only of the employees of the embassy, but also of its visitors, while ensuring the security of the embassy.

Controls were also performed in large shopping malls, as well as small stores. Controls took place in a gallery, central supervisory authority, prison, schools and kindergartens, and restaurants.

The above overview indicates that personal data processing by means of video surveillance systems is utilized in almost all conceivable life situations and, in the eyes of a number of citizens, these systems are becoming an absolutely common part of our lives and a major issue for our society. The acquired recordings are being used to furnish proof in neighbourhood disputes or to demonstrate disciplinary misconduct of children at school. They are often misused in companies to check the attendance and performance of working tasks, with potential consequences under labour law for the monitored persons.

Therefore, the Office welcomes a resolution taken by the Government of the Czech Republic that the use of video surveillance systems should be regulated in our legislation.

CHIP CARDS

A control concerned with the use of chip cards with the RFID technology was carried out in 2009 in a bus transport company, which operates both a city transit system and transport for the entire region. At the same time, the company allows other transport companies to use its technology within the regional integrated transport system.

The company enables passengers to obtain prepaid coupons or time-limited coupons only in the form of chip cards. The cards are equipped with a chip containing the RFID technology, i.e. a technology of contactless transfer of data. Within the entire system of offers of prepaid coupons, the company issues personal non-transferable cards for adults, students, pupils and seniors. The company also offers an anonymous transferable card called a "family card". Apart from the family card, the other cards are used as normal prepaid tickets. The card contains a copy of the holder's photograph and his name and surname. Each card is identified by a unique number and the individual types are mutually distinguished by colours and graphic design. The company requested that the applicant provide, in his application for a card, in addition to his name and surname, also his date of birth and place of residence. From those passengers who were entitled to one of the discounts based on the transport terms, it also required the relevant certificate, e.g. on study. The family card is not labelled and is used de facto as a wallet.

The card holder was entitled to use prepaid transport services. The means of transport were equipped with RFID chip readers. According to the type of the fare, either funds were deducted from the aggregate financial limit or the validity of the prepaid time coupon was checked. The readers recorded information related to the specific card. This included the number of the card, date and time of boarding, place of boarding and place of disembarking. Furthermore, information on deduction from the financial limit was recorded for prepaid coupons. The company further supplemented this information by information from the machines for recharging the coupons. The database containing the identification details of the card holders was kept separately from the databases on transport transactions. All the transactions connected with the use of chip cards took place on the basis of the unique card number. Mutual settlement of the costs related to the provision of transport services by other transport companies also took place through the clearing centre exclusively on the basis of the unique card number. The company maintained all this information on the specific card holders and transaction information for a period of five years. In this case, the control concluded that the company, as the holder of the database where the identification personal data of the chip card holders were stored, also had at its disposal information on financial transactions, information on the specific place and time of boarding and disembarking by the specific passenger. For its own needs, the company utilized only information on the use of the integrated transport system for commercial and marketing purposes. It did not utilize, for its activities, information on use of transport by a specific person. However, in several cases, it submitted this information concerning a specific natural person to a competent governmental authority based on its statutory duty.

The control demonstrated that, except for pupils, who had no personal identity card, it was not necessary to process identification personal data for the company's own activity. Each non-transferable card contains a copy of the holder's photograph and his name and surname, as well as the date of birth. Based on the statutory authorization, a person appointed by a transport company may control, in addition to the ticket, also the identity of the passenger on the basis of his personal identity card (under the conditions stipulated by the relevant regulations on passenger transport). On the basis of this conclusion, the inspector imposed a remedial measure on the transport company, the obligation to destroy the database of the chip card holders. The company would be authorized to process identification personal data of the card holders only when the card holder applied for a duplicate as a result of loss or theft of the card and gave his explicit consent to this effect. This also applies analogously in respect of children, who do not possess their own personal identity card thus cannot be checked in any other way. **The controlled company accepted the conclusions of the inspection.**

SECTION SPEED CONTROL

The controlled entity was the Capital City of Prague, the Municipal Police.

The equipment designated for speed control determines the section speed of vehicles as a ratio of the known constant distance between two measuring profiles to the time required for travelling this distance. Each measuring device consists of a control unit (computer) for each pair of cameras (C1 and C2) and a database server. The equipment operates in that the individual detection devices (cameras) continuously monitor the situation in the given lanes within the set measuring profiles. The measuring profiles are set at a certain fixed distance from each other (approx. 500 m) on the road and thus delimit the measured section. The control unit detects vehicles and their license plates in the visible field of the camera and then reads the license plates. The devices are equipped with HDTV cameras that provide substantially better picture quality compared to normal cameras with TV definition. This ensures high reliability of the detection of vehicles, easily legible license plates and better quality of documentation of the driver's face. The recordings obtained by camera C1 upon entry of the given vehicle to the measured section and camera C2 upon its exit are stored in the central data storage system (technical equipment – server). If the equipment detects any exceeding of the set speed, it sends the recording consisting of the photograph of the vehicle, including the driver and passenger on the front seat, and digitalized license plate (camera C1), digitalized license plate (camera C2) and information on the speed of the vehicle, to the storage system of the Municipal Police for further procedure on the misdemeanour. The actual measurement is thus absolutely automatic and cannot be affected. The accuracy of the measurement is guaranteed by the fact that the distance between the measuring points is measured with high accuracy and both pictures contain accurate time stamps based on a stable time base. The parameters of the measurement can be administered by remote access and set through a suitable interface, if appropriate. This includes, e.g., setting the maximum speed limit, the values of speed qualified as a misdemeanour (tolerance field), etc.

Video surveillance systems that detect cases of running a red light are set so as to obtain photographs of the drivers entering the intersection when the traffic light is red.

18 section speed measurement devices and 9 systems monitoring cases of running a red light were installed in Prague at the time of the control.

Section measurement systems are installed on the basis of a report of the Police of the Czech Republic, which determined, in its communication dated December 31, 2008, the location of technical means for speed measurement. However, this method of measuring speed simultaneously processes the personal data of persons who have not committed any misdemeanour and, therefore, this continuous measurement of all passing vehicles constitutes a strong interference with the privacy of individuals and its use must be based on actual danger related to the given section, requiring permanent supervision. The Office is not competent to assess the justification of selection of the given places.

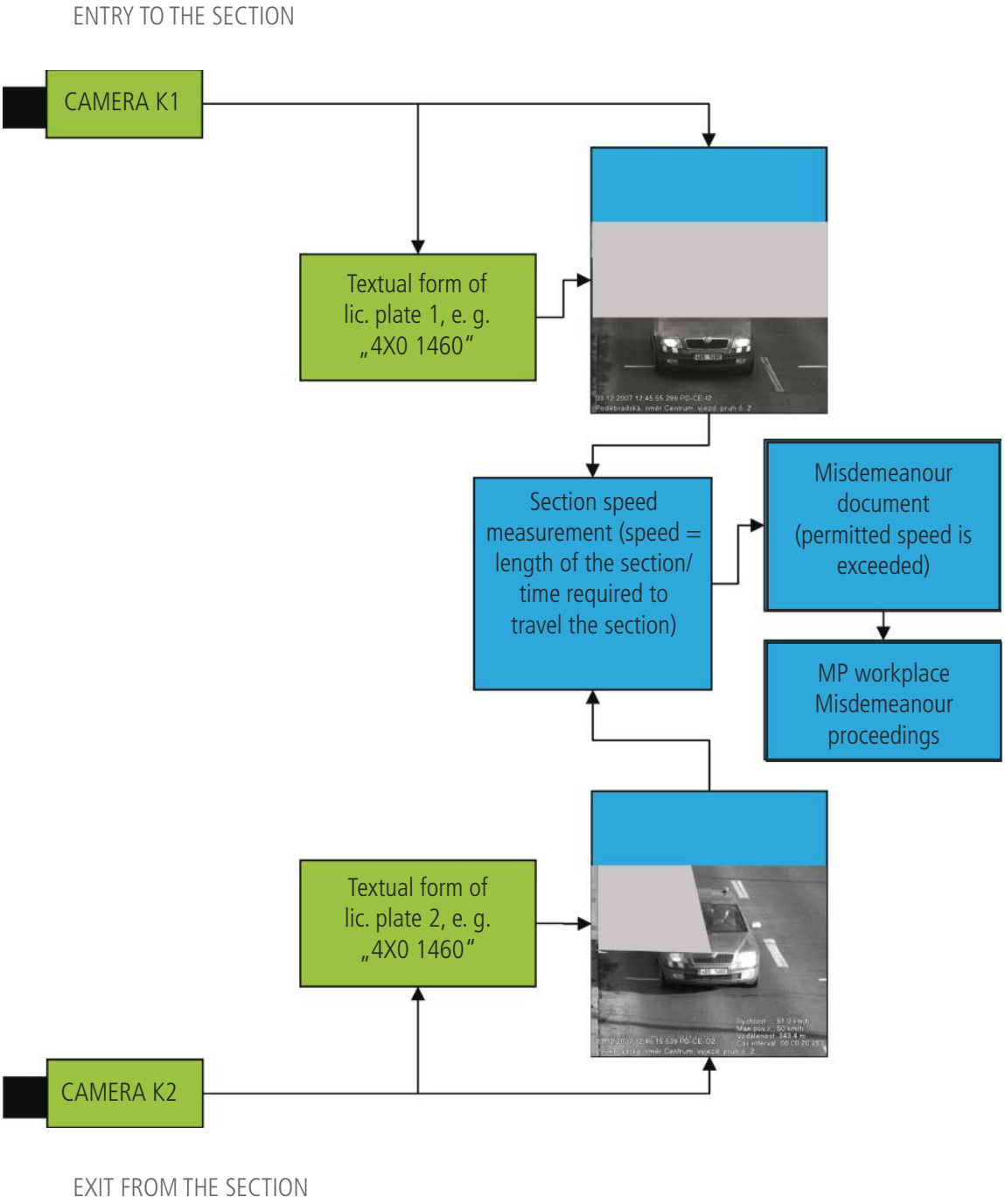
The controlled entity is a controller of these data and maintains the data for an appropriate period of time corresponding to the Misdemeanours Act.

Within the control, the inspectors imposed the duty to entirely remove the image of a passenger on the front seat, instead of the disputable blurring of his face on the photograph.

Information from the mentioned video surveillance systems is processed by the Police of the Czech Republic in unmodified form within the central data storage system. The Police of the Czech Republic is also the controller of these data within the meaning of Act No. 101/2000 Coll.

Speeding ticket scheme: functions of the system

It follows from the properties of the speeding ticket scheme that the following data are inserted in the document on the misdemeanour in the event of excess speed beyond the permitted limit: the image from camera C1, where only the license plate is visible, and the image(s) from camera C2, where a passenger on the front seat is not visible.



Description of the UnicamPRIVACY software

Modification I – Covering part of the image from camera C1

The image from camera C1 at the entry to the given section is modified, for the purposes of measuring speed, in that part of the image above the license plate is blurred as indicated in the picture.

Example of modified images from camera C1

Only for the needs of the Police of the Czech Republic

Figure 1: Picture S1 taken by camera C1

Only for the needs of the Municipal Police

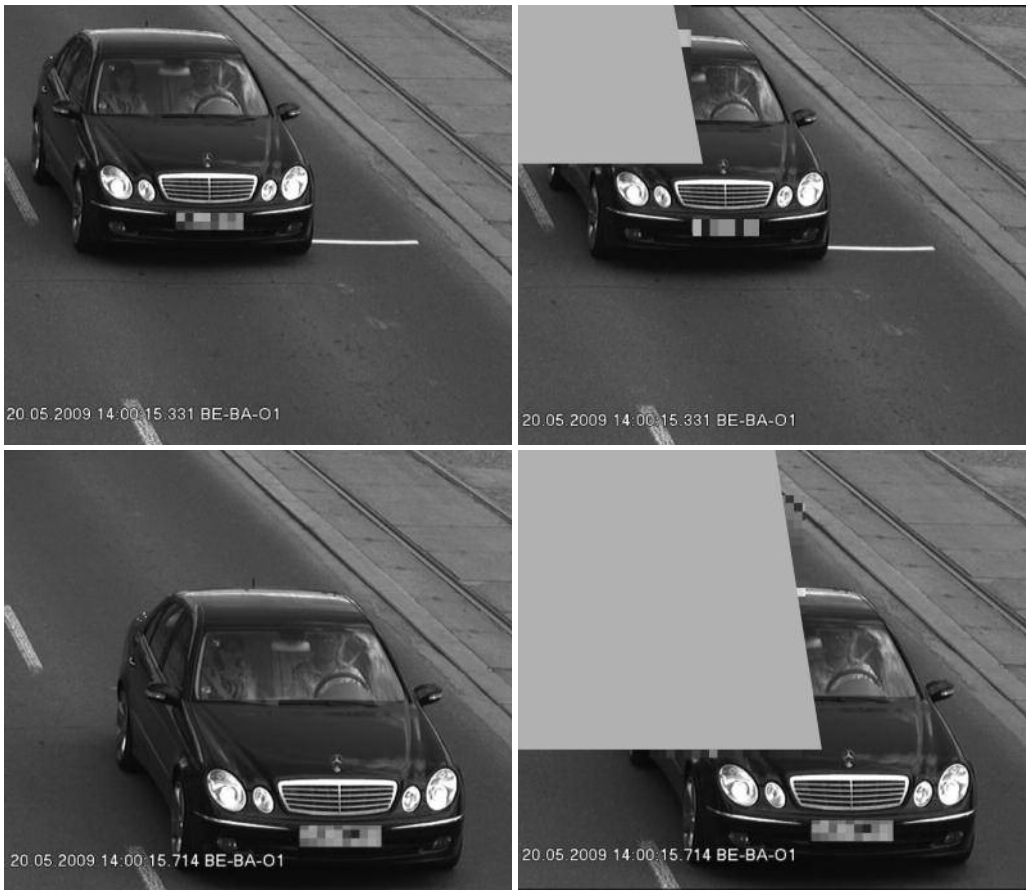
Figure 2: Modified picture US1 – automatically modified so as to retain only those attributes that are necessary to demonstrate the potential misdemeanour – legible license plate 1 and line on the road, but without the possibility to identify the driver or the passenger

Technical solution:
Based on location of the license plate, the blurred area above the license plate is defined.

Example of modified images from camera C2

Only for the needs of the Police of the Czech Republic

Only for the needs of the Municipal Police



Figures 3 and 4: Images S2 taken by camera C2

Figure 3: Modified pictures US2 – automatically modified so as to retain only those attributes that are necessary to demonstrate the potential misdemeanour – legible license plate 2, line on the road and face of the driver, but without the possibility to identify the passenger

Technical solution:
The area that is covered-over in the left half above the front of the vehicle, corresponding to the part of the vehicle with the passenger, is defined on the basis of the location of the front of the vehicle with the headlights.

INTERNET

The circumstances and the way in which the Internet was developed are generally known; the problem lies in the fact that its development was not really monitored by anyone and no one set any rules. Today both their absence and attempts to introduce them are widely criticized.

The Internet contains vast quantities of information. A considerable part of this information is related to identifiable persons and thus constitutes personal data. Not every computer processing of the individual bytes within the basic computer functions can be considered to be automated processing of personal data within the meaning of the Personal Data Protection Act, which is subject to registration with the Office; this rather needs to be an organized activity involving a complex of information complying with the criteria for personal data. Only upon creation of comprehensive information may the conditions for identifiability be created. Indeed, information on the Internet pertaining to identifiable persons can be based on private law. As follows from Award of the Constitutional Court File No. I. ÚS 4/04 dated March 23, 2004, *"criminal law and the related qualification of certain conduct that is based on private law as a criminal offence must be considered ultima ratio, i.e. the last legal resort that is relevant particularly for the entire society, i.e. from the viewpoint of protection of the fundamental social values. However, in principle, it cannot serve as a means replacing protection of the rights and legal interests of an individual in the area of private-law relations, where it is particularly up to the given individual to protect his rights which are subject to judicial protection. Nevertheless, it is unacceptable for this protection to be actively provided by prosecuting bodies, which should aim to protect primarily values common for the entire society, rather than directly specific rights of an individual, which are based, in their nature, on private law."*

In these cases, it is appropriate to apply civil-law protection of personal rights under the Civil Code. Where an individual fails to act with a view to protect his rights or where the statutory instruments serving to protect the rights of individuals are not sufficiently effective, these measures cannot be replaced or supplemented by criminal or administrative law. Indeed, pursuant to Article 13 of the Civil Code, a natural person has the right to claim that other persons refrain from unauthorized interference with the right to protection of his personal rights, that the consequences of such interference be remedied and that he be provided with appropriate compensation. A similar approach was adopted by the Supreme Court in its ruling 30 Cdo 3070/2006 of December 21, 2006, concerning personal data set out on the "kadran.cz" website.

The "Lindquist" case is very important in the area of personal data processing on the Internet.

However, it would probably be absurd and practically unfeasible to prevent specification of the names of various persons, references to their work or hobbies on the Internet without their express approval. This would mean that it would not be possible to mention other people in blogs, journalists would be unable to mention anyone in their articles, companies could not mention their members, publishers could not state the authors, fans would not be able to mention singers or actors ... unless they had their express consent. Each such case of processing would have to be registered with the Office before its commencement. This would mean that everyone would be forced to notify the Office in advance that he intends to write an article where he will mention a specific person. Such a procedure would surely be inappropriate and practically unfeasible.

Responsibility for information disseminated through the Internet

It is difficult to find the person responsible for information that can be found on the internet and there are many instruments supporting anonymity. Therefore, both in the EU and in the U.S.A., the responsibility is transferred to the provider of services of the information society, i.e. the server administrators. Indeed, the necessary connection data can be ascertained only in case of investigation of a crime, pursuant to Article 97 of the Electronic Communications Act. However, in case of a misdemeanour or administrative offence, the provider of the service of the information society

(webhosting, provider, ...) is not authorized to disclose the necessary information. Consequently, this problem is also relevant in those cases where the administrative authority knows the identity of the author, i.e., e.g., where the author publicly acknowledges his work and where administrative proceedings without objective findings of fact need not bring the desirable result. It is very difficult to determine the identity of the controller from the viewpoint of the Personal Data Protection Act, i.e. the person who determined the manner and means of processing.

Certain options are again provided by the Act on Certain Services of the Information Society, namely Article 5, which stipulates the *"Responsibility of the Service Provider for Storing the Contents of Information Provided by the User"*:

"(1) The provider of a service consisting in storage of information provided by the user shall be responsible for the contents of the information stored at the user's request only in those cases

a) where the provider could know, with respect to the object of his activities and the circumstances and nature of the case, that the contents of the stored information or the user's conduct is illegal; or

b) where the provider demonstrably learned about the unlawful nature of the contents of the stored information or the illegal conduct of the user and failed to take all the steps that could be reasonably required of him, without delay, to remove or block access to such information.

(2) The service provider set out in paragraph 1 above shall always be responsible for the contents of the stored information in those cases where the provider directly or indirectly exercises decisive influence over the user's activity."

Thus, the actual provider of the mentioned service, who is undoubtedly a processor pursuant to the Personal Data Protection Act, has no direct responsibility for the contents and needs to be effectively informed of the unlawfulness of the contents of the given website or conduct of the users. Services of the information society should be defined at this point. The cited Act stipulates this definition in Article 2 in that a service of the information society is any service provided by electronic means on the basis of an individual request of the user lodged by electronic means, usually provided for consideration; a service is provided by electronic means if it is sent through an electronic communications network and collected by the user from the electronic equipment for data storage. Electronic means include particularly the network for electronic communications, electronic communication equipment, terminal telecommunication equipment and electronic mail.

Service provider means every natural person or legal entity that provides a service of the information society and user means every natural person or legal entity that utilizes a service of the information society, particularly for the purpose of seeking or making available information. It follows from the above that this includes services such as "hosting", i.e. the provision of a disk capacity with possible remote access. Consequently, this includes not only websites, but also various shared data such as image galleries, various videos, etc. In this relation, information needs to be understood as data, as this is not information guaranteed by the Constitution, but rather data that are frequently a business article. For example, if you buy certain data in an e-shop (program, music, etc.) and have the data sent to you, e.g. burnt on a CD, this is a classical business transaction; however, if you have them sent by e-mail or download them from the Internet, this is a service of the information society.

The service provider should have a contractual option of terminating the provided service in case of the suspicion of unlawful contents. This aims to avoid potential business disputes in the event that the data are removed or blocked.

UNSOLICITED COMMERCIAL COMMUNICATIONS

Statistics – unsolicited commercial communications – for 2009:

Instigations (complaints) related to dissemination of unsolicited commercial communications	2261
Instigations (complaints) related to dissemination of unsolicited commercial communications resolved	1678
Unjustified instigations (complaints) – an unsolicited commercial communication not involved or an unsolicited commercial communication or spam from abroad	266
Cases where the sender was not found	91
Controls initiated (number of controlled entities)	145
Controls completed	131
Number of entities on which a remedial measure was imposed	456
Number of administrative proceedings	112
Total amount of fines imposed in these administrative proceedings	CZK 797,000

Compared to the previous year, when the number of complaints raised about dissemination of unsolicited commercial communications reached approx. 1,500, this number markedly increased in 2009, by roughly one third. There could be several causes.

One of them could lie in the fact that this method of communication (sending unsolicited commercial communications by electronic means) is still effective for companies and this is tolerated by the addressees of unsolicited commercial communications. Another reason, which we have discovered in our control activities, consists in the fact that the same entrepreneurs are no longer indifferent to receiving unsolicited commercial communications, particularly after being themselves punished by the Office for sending such communications.

Another reason for the increase could lie in the new phenomenon of internet communication, which substantially increased this year, i.e. "viral marketing". This operates on the principle of "forwarding". The offers are thus transferred by people themselves (a human chain). This aims to increase sales, extend the business potential and raise awareness of the brand, while expending minimum costs. To make them effective, these offers take the form of various games, amusing videos or audio files, where the addressee discovers the offer or company promoted only at the end. Pursuant to the Act on Certain Services of the Information Society, 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 who performs a regulated activity or is an entrepreneur pursuing activities that are not regulated; commercial communications also include advertising pursuant to the special regulation." Consequently, viral marketing undoubtedly involves a commercial communication. However, there is an issue related to the identity of the sender. Indeed, only the sender, rather than the person for whom the commercial communication is intended, can be punished for sending unsolicited commercial communications. The latter could be the case, e.g., in cases of forwarding, where the first addressee grants the given company his consent to sending commercial communications; in that case, this is not an unsolicited commercial communication. The recipient then forwards the message (commercial communications) within normal correspondence amongst his relatives, colleagues, friends ... and the company for whose benefit the communication is thus disseminated cannot be punished.

However, the situation is different in terms of another method or technique of viral marketing, which entails web invitations, where the companies' websites contain links such as "send to your acquaintance", "recommend to your friend" ... After clicking on the link, an offer of the given company is displayed and this can be immediately sent. From the viewpoint of the Act on Certain Services of the Information Society, these cases are relatively straightforward. Pursuant to Article 3 of the cited

Act, the service provider is responsible for the contents of the transferred information only in cases where:

a) he himself initiates the transfer;

b) he chooses the user of the transferred information; or

c) he chooses or changes the contents of the transferred information.

Consequently, this method of viral marketing corresponds to the third variant, since the sender initiates the transfer and chooses the user, and the contents are already previously prepared by the company itself. Responsibility is thus borne both by the sender and by the company for whose benefit the offer is sent in this way.

ADDRESSING COMPLAINTS AND PROVISION OF CONSULTATIONS

The increasing trend in the number of inquiries, requests for a legal opinion or statement, instigations and complaints of the citizens invoking the Office's supervisory competence continued in 2009. The Public Relations Department was forced to optimize its working procedures and provide the initial legal assessment of the contents of the pleadings from the viewpoint of breach of the duties in personal data processing and provision of consultancy only when this was strictly within the competence of the Office. Previously, the consultations and replies provided by the Department were very often initially adapted to the needs of the inquiring parties. Particularly law firms requested, on behalf of their clients, assessment of often very complex legal issues connected with the business relations of legal entities, which are not subject to Act No. 101/2000 Coll.

In telephone inquiries, qualified and structured responses were usually requested in connection with cases of protection of personal data covered by the media, which placed enormous demands on both the time of the individual officers and their professional expertise. In the end of 2009, it was therefore necessary to inform the public through a communication published on the Office's website that only basic general information would be provided by telephone and that any further procedure by the applicant would have to take particularly written or electronic form, or the form of a personal consultation.

Of 62 personal consultations provided in 2009 to governmental authorities, local governments, legal entities, natural persons, both operating a business a not operating a business, in the position of personal data controllers and processors, their employees and also data subjects, we mention the most important clients for illustration: the Ministry of Foreign Affairs, Ministry of Finance, Ministry of the Environment, Ministry of Industry and Trade, State Office for Nuclear Safety, Czech Statistical Office, Czech Mining Authority, LIDL Česká republika, v.o.s., Centre for Determining Results of Education, National Institution of Technical and Vocational Education and Czech Office for Standards, Metrology and Testing.

In spite of the continuing increase in the number of inquiries received (1 934 inquiries were answered, compared to 1 778 in 2008), the average time required for responding to the inquiries equalled two weeks. It should be noted that the relevance of the inquiries and requests for assessment of the presented projects continued to grow; the most extensive projects included: keeping records in relation to a contemplated issue of governmental bonds; testing a database of passports with biometric data; use of body scanners operating on the principle of ionizing radiation at airports; and various types of internal regulations issued by personal data controllers in relation to the duties stipulated in Article 13 of Act No. 101/2000 Coll.

A total of 879 instigations for initiation of proceedings ex officio were dealt with, which corresponds to an increase by 26% compared to 2008. The most significant increase was recorded in the number of pleadings rejected as unjustified, twice as many complaints were referred to the substantively com-

petent governmental authorities, while there was a relatively marked decrease in the number of complaints referred for further analysis prior to commencement of control (by 36%). A common reason for this state of affairs lay in the fact that many complaints, often similar in their nature, did not give rise to a justified suspicion of violation of Act No. 101/2000 Coll. Anonymous pleadings were usually rejected, except for those complaints that indicated a justified concern of the complainant about possible punishment by the personal data controller, which was typical mainly of employment relations, including a realistic threat of losing a job. Furthermore, the Office took into consideration the scope of the databases of personal data and the likelihood that the defective activity would be repeated by the controller or processor.

Statistical data on complaints addressed in 2009:

Total	879
of which:	
submitted for control	129
submitted for commencement of proceedings	43
forwarded to the competent bodies	24
suspended with notification	683

The citizens, being in the position of data subjects, were again often concerned in 2008 about video surveillance systems (over one fourth of the total number of complaints), publication of personal data on the Internet and processing of sensitive personal data in health care. Although separate chapters of the Annual Report are dedicated to these aspects, we consider it necessary to mention several observations.

The Office was forced to deal with a number of complaints (36) related to operation of video surveillance systems by private individuals, i.e. within the regime of Article 3 (3) of Act No. 101/2000 Coll. (hereinafter the "Act"). Unless abuse of the recordings for a purpose other than that declared, being predominantly protection of own property, was proven, including the provision of the relevant recordings to the prosecuting bodies, the complainants were referred to the Civil Code for resolution of their neighbourhood disputes. A relatively complicated issue is associated with the right of data subjects to information pursuant to Article 12 of the Personal Data Protection Act, or the right to direct inspection of the recordings, without simultaneously affecting the rights of other persons recorded by the video surveillance system. Where the operator of the video surveillance system proceeds pursuant to Article 5 (1) (e) of the Act, the relevant recording will usually have already been deleted. Indeed, Article 12 of the Act cannot serve as a basis for inferring the duty to maintain the recording for the reason of resolving requests from the data subject for longer than required to attain the set purpose (usually several days). The duty to provide information stipulated in Article 11 of the Act may be fulfilled by the controller even without actually making the recording from the camera system available.

The most pressing issue connected with publishing personal data on the Internet lies in the fact that it is virtually impossible to secure the data at the level required by Article 13 of the Act. Similar to video surveillance systems, the Office did not interfere with relationships that could be resolved under private law. This was true of cases where personal data were obtained and subsequently published only once, often accidentally. In contrast, where information leaked from a database of systematically processed personal data, the liability of the controller for its leakage to the Internet was entirely clear and these cases where resolved within the supervisory competence of the Office. A special problem consists in the requirement for secured communication, which includes, with effect from November 1, 2009, the information system of data boxes. The Office replied to frequent questions on this subject in the sense that it did not yet possess knowledge in terms of possible justification of the failure to use these boxes in with reference to the principles of protection of personal data, naturally provided that

they are operated in accordance with the special law, i.e. Act No. 300/2008 Coll., on electronic acts and authorized conversion of documents.

The most frequent subject of inquiries and complaints in 2009 consisted in collection of personal data that were redundant for the given purpose, particularly by mobile operators, in the form of acquiring copies of identity cards, which is regulated by Act No. 328/1999 Coll., on identity cards, as amended. Although violation of Article 2 (6) of the cited Act is a misdemeanour, which falls within the competence of municipal authorities with extended competence, this also results in breach of the duty to collect personal data only to an extent necessary to attain the set purpose, which is not true, in this case, e.g., of photographs of the client or the personal data of his relatives. Therefore, the Chairman of the Board of Directors of one of the entities having a contracting obligation in the provision of telecommunication services was requested, through a personal letter from the President of the Office, to provide for a systemic remedy. Unfortunately, the defective state of affairs continues to persist, including requests for making copies of other personal documents, mostly the driver's license, which is absolutely irrelevant in conclusion of a contractual relationship, since citizens are obliged to prove their identity through their identity cards. The Office will also deal with this subject next year.

FINDINGS FROM ADMINISTRATIVE PROCEEDINGS

PROCESSING DNA PROFILES IN THE NATIONAL DNA DATABASE

As the use of genetic information is becoming ever more common, the Office is encountering issues related to processing these sensitive data with increasing frequency. In 2009, the Office again dealt, in this area, with the aspects of maintaining DNA profiles by the Police of the Czech Republic within the National DNA Database, and specifically assessed the case of a complainant who was convicted of an especially serious economic crime and whose DNA sample was obtained during collective sampling, when the Police of the Czech Republic performed buccal swabs in respect of all persons who were serving imprisonment for an intentional crime at that time.

Given the absence of adequate legislation on the use of DNA in the activities of the Police of the Czech Republic, decision-making in similar cases is relatively difficult as it is always necessary to individually assess and apply the highly general legal rules on which the National DNA Database in the Czech Republic is based. Nevertheless, in these cases, the Office can rely, in its arguments, inter alia, on judgment of the European Court of Human Rights in S. and Marper v. The United Kingdom (ruling of the Grand Chamber Ref. No. 30562/04 and 30566/04 of December 4, 2008; hereinafter the "ECHR" and "ECHR ruling"). In this ruling, the ECHR noted that the mere retention of a DNA profile constitutes infringement of the right pursuant to Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, regardless of whether or not the information is further used. Such infringement is justified in a democratic and legal State only subject to setting clear, sufficiently specific and restrictive rules stipulated by a law. Furthermore, the ECHR considers it absolutely fundamental that the domestic law afford appropriate safeguards to prevent any abuse of personal data, where the need for such safeguards is all the greater where the protection of personal data undergoing automated processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The above considerations are especially valid in respect of sensitive genetic data (i.e. data obtained by DNA analysis).

At the same time, it must be pointed out that, in similar cases, the Office deals with the issue of retaining a DNA profile in the National DNA Database, rather than with the justification of or need for taking a biological sample in connection with investigating a specific crime. In the opinion of the Office, these two situations must be consistently distinguished, as further retention of a DNA profile pro futuro aims at an entirely different purpose than the taking and use of a sample in connection with investigating a specific crime.

Based on the wording of Act No. 273/2008 Coll., on the Police of the Czech Republic (effective from January 1, 2009; hereinafter the "Police Act") and the cited ECHR judgment, the Office followed in this case from the fact that the Police Act does not encompass any express authorization to create and enter data into the National DNA Database and authorizes the police officers to process sensitive personal data (i.e. also a DNA profile) without consent only where this is necessary for the performance of tasks of the Police of the Czech Republic; however, it does not define the word "necessary".

On the basis of these facts, the Office came to the conclusion that the Police Act did not contain clear and sufficiently specific rules for processing personal and sensitive data in the National DNA Database. The Office must replace the lacking clear statutory rules by interpreting the general terms of the Police Act based on the Convention for the Protection of Human Rights and Fundamental Freedoms, case-law of the ECHR and also Recommendation No. R (92) 1 of the Committee of Ministers to Member States (of the Council of Europe) on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system. Pursuant to Art. 8 of the Recommendation, the results of DNA analysis and the information so derived may be retained where the individual concerned has been convicted of serious offences against the life, integrity and security of persons. Since the case at hand involved an economic offence, which does not fall within this definition, which is considered by the Office to be a fundamental guideline (in the absence of any other legal regulation) for strict interpretation of the authorization of the Police of the Czech Republic to retain DNA profiles in the National DNA Database, the Office came to the conclusion that inclusion of the relevant DNA profile in the National DNA Database violated the Personal Data Protection Act.

While in its decisions in similar cases the Office does not question the legitimity of the existence of the National DNA Database, it nevertheless consistently requires that this instrument be used only subject to fulfilment of the precondition of necessity of processing sensitive data for the performance of tasks of the Police of the Czech Republic. Indeed, in view of its competence, the Office cannot allow that the necessity of retaining DNA profiles in the database be automatically declared, e.g. with respect to every intentional crime, the more so without any unambiguous statutory authorization.

PUBLISHING PERSONAL DATA BY MUNICIPALITIES

In relation to the performance of its supervisory competence, the Office has repeatedly encountered the issue of publishing personal data within the activities of municipalities, whether in delegated or in independent competence. The Office is aware that the municipalities must fulfil the requirements for transparent performance of their activities and, at the same time, respect the rights to privacy of the affected persons, which could be a difficult task in the labyrinth of legal regulations. In the interest of preventing violation of the Personal Data Protection Act, the Office expresses its opinions on various aspects of personal data processing by municipalities within its statements and other texts published particularly on its website. Nevertheless, in a situation where infringement on the rights protected by the Personal Data Protection Act has been ascertained and demonstrated, it is necessary to impose a penalty on the given municipality within administrative proceedings, even though, after almost 10 years of existence of the Office, the fines in this area continue to be more or less symbolic.

The Office is of the opinion that, in publishing information, it is necessary to thoroughly consider the risks connected with publication of personal data (i.e. information that can often considerably

interfere with the privacy of individuals) in the media and particularly on the Internet, where information can be sought-out even long after its publication.

The aspects of publishing personal data by municipalities which were dealt with by the Office in 2009 can be divided into several areas:

Draft agenda of a meeting of the municipal assembly
Dealing with pleadings by the citizens (applications, complaints or instigations)
Resolutions from meetings of the municipal assembly or council
Acts of the municipality in administrative proceedings
Provision of information in the municipal journal

Draft agenda of a meeting of the municipal assembly

One of the duties aiming at increasing the transparency of the activities of municipalities is stipulated in Article 93 (1) of the Municipalities Act, according to which the municipal authority shall provide information on the place, time and draft agenda of a future meeting at least 7 days in advance. This information should be posted on the official board of the municipal authority and, if appropriate, it may also be published in some other way usual in the given municipality. It is clear that meetings of the municipal assembly will very often discuss issues that are concerned with specific natural persons and such meetings will thus necessarily entail personal data.

Provision of information on the draft agenda of a meeting of the municipal assembly is a statutory duty, which aims primarily, in the opinion of the Office, to provide information on the activities and plans of the municipalities, i.e. on the matter that will be discussed, rather than on the persons whom the matter concerns. Article 93 of the Municipalities Act does not stipulate any explicit duty to publish the personal data of those with whom the matters at hand are concerned within the information on the draft agenda. Under these circumstances, it should be concluded that publication of personal data is not required in order to comply with this duty. Thus, in the opinion of the Office, in accordance with the Personal Data Protection Act, the municipality must state, within the draft agenda (where the given item concerns a specific natural person), either only a description of the case or initials of the name and surname and municipality of residence (or part of the municipality, but not the exact address).

The above is analogously also true of any publication of documents that are to be discussed and that contain personal data of, e.g., applicants or complainants. From the view of the Personal Data Protection Act, it is irrelevant whether personal data are published in the form of information provided by the municipality or directly by publishing the given (e.g. scanned) deed.

Of course, all information (including personal data) can and must be presented at the meeting of the assembly as such. This different approach is based on the fact that, in the phase of publishing the draft agenda, all the information is disclosed to an unlimited circle of persons (particularly through the Internet), i.e. also to persons who are absolutely disinterested in the matter.

This issue is further dealt with by the Office on its website in the section Opinions of the Office – On practical issues.

Dealing with pleadings by the citizens (applications, complaints or instigations)

An important part of activities of municipalities undoubtedly consists in dealing with various instigations, complaints, petitions or applications of the citizens. Apparently in an attempt to ensure that the procedure in dealing with various pleadings is as open as possible, municipalities publish various cases (particularly disputable issues, such as disagreement with a construction plan or complaint about non-compliance with the municipality's contractual obligations) on its website or in the local press. This again often entails personal data processing, as the citizens addressing the municipality are usually identified, in their pleadings, by their name, surname, address of residence, and possibly also the date of birth or even the birth number.

In connection with dealing with pleadings by the citizens, the applicable legal regulations (particularly the Municipalities Act, as well as, e.g. the Code of Administrative Procedure) do not

provide any legal title, i.e. authorization, to publish the personal data contained in the given pleading. Thus, based on the requirement set out in the introductory part of Article 5 (2) of the Personal Data Protection Act, such personal data processing requires the consent of the affected persons. However, this procedure will be possible only in certain cases; anonymisation of personal data will be a more frequent and probably also more suitable method. In other words, in a situation where a municipality considers it necessary to provide information to the general public on pleadings submitted by citizens, this is possible – with respect to the objective of this step, i.e. ensuring transparency of the matter at hand, rather than the persons concerned – to do so by publishing anonymised information, or even the pleading itself, where the personal data are consistently rendered illegible.

Resolutions from meetings of the municipal assembly or council

The Office already provided its opinion on the aspects of publishing resolutions from meetings of municipal bodies (assembly and council) and extracts from these resolutions in its statement No. 2/2004 – Disclosing and publishing personal data from meetings of municipal and regional assemblies and councils (cf. www.uoou.cz/Názory Úřadu/Stanoviska). The application of duties stipulated by the Personal Data Protection Act in this area must be based on consistent distinguishing of the right to participate in a meeting of the municipal body, or the right to inspect the minutes of meetings, and the right to obtain information on the activities of the municipality.

The Municipalities Act explicitly defines the scope of persons authorized to participate in the meetings of municipal assemblies (council meetings are not open to public) and the scope of persons who have the right to inspect resolutions from the meetings. Specifically, this includes citizens of the municipality, natural persons that own a real property located in the jurisdiction of the municipality, and also foreign nationals who are registered for permanent residence in the municipality if so stipulated by an international treaty binding on the Czech Republic and promulgated (Articles 16 and 17 of the Municipalities Act). On the basis of the Municipalities Act, this scope of persons is entitled to become acquainted, either directly at the meeting of the assembly or by inspecting the minutes of the meetings of the council or assembly, with the entire contents of the meeting, i.e. the contents of all the documents concerning the discussed matters, including the personal data of persons with whom the meeting was concerned. This procedure is in conformity with Article 5 (2) (a) of the Personal Data Protection Act and does not require the consent of the affected persons.

However, the situation is different in respect of disclosing information on the activities of the municipality to the general public, particularly on a website or in the press. The duty of the municipality to proceed transparently and provide information on its activities follows both from the Municipalities Act and from the Act on Free Access to Information. However, in this case, information is disclosed not only to the above-specified range of persons strictly defined by the law (citizens of the municipality), but de facto to an unlimited number of recipients. However, a fundamental difference compared to the above-described situation lies in the purpose of publication of information by the municipality, i.e., in this case, transparent execution of State administration and local government, rather than provision of information on specific persons whose matters were discussed. Indeed, in the Act on Free Access to Information, this principle is explicitly reflected in Article 8a of the Act, according to which personal data do not fall within the scope of this Act. In this case, personal data may be published (e.g. within the minutes of a resolution from a municipal council's meeting on the website) pursuant to the Personal Data Protection Act only with consent of the persons with whom the data are concerned. However, it will probably be more practical to render the published data anonymous. In general, it can be stated that, from the viewpoint of the requirements for personal data protection, it is admissible to specify the initials of the name and surname and the municipality or its part.

Acts of the municipality in administrative proceedings

Administrative proceedings pursued by municipalities sometimes result in a situation where a certain document has to be served by publication on the official board or the electronic official board on the municipality's website. This may be true of proceedings with a large number of parties, where documents may be served through a public edict in accordance with Article 144 (5) and (6) of the Code of Administrative Procedure. The thus-served (published) documents must have all the prescribed requisites and will thus also contain the personal data of all the parties. Publication of personal data in this manner is an activity envisaged and permitted by the law and is thus in conformity with Article 5 (2) (a) of the Personal Data Protection Act.

However, further duties stipulated by the Personal Data Protection Act must also be fulfilled at the same time, i.e. particularly the duty to process personal data only for a period required for the purpose of their processing, or to process personal data only in accordance with the purpose for which they were collected. Consequently, if a document is considered to be served, pursuant to Article 25 (2) of the Code of Administrative Procedure, on the fifteenth day after its posting, this is also the period required for publication of the personal data. After expiry of this period, the publication in the given manner must be deemed to constitute personal data processing for a period longer than necessary.

Provision of information in the municipal journal

In a number of municipalities, the municipal journal is the main source of information on the activities of the municipality and its bodies. In general, it can be stated that publication of personal data in this way is subject to the same considerations as set out above in relation to the Internet, because, in spite of its much narrower scope, a municipal journal must also be considered to be a medium accessible to an unlimited circle of recipients.

Similar to the issue of publishing personal data in connection with important life occasions, which was highly discussed in the past, other cases of publication (e.g. publication of persons who have failed to return books borrowed from a public library) are also based on the fundamental principle of personal data protection, i.e. the requirement for existence of a legal ground for their processing. This legal ground consists either in consent of the affected persons or in a procedure conforming to one of the exemptions pursuant to Article 5 (2) (a) to (g) of the Personal Data Protection Act; in a vast majority of cases, the consent of the given persons will be required.

Personal data processing within various registries is either a duty stipulated directly by a law or a necessity without which a certain service (such as a public library) cannot be operated. However, it is always necessary to consistently comply with the principle set out in Article 5 (1) (f) of the Personal Data Protection Act, i.e. the duty to process personal data only in accordance with the purpose for which they were collected. Therefore, personal data required for the provision of services by a municipality cannot be automatically published, as this would constitute processing of the data for a different purpose.

In relation to publication of personal data as a consequence of various relationships following from non-compliance with contractual obligations, the Office often encounters the argument that the publication of a debtor is a procedure conforming to Article 5 (2) (e) of the Personal Data Protection Act, i.e. a form of protection of the rights of the given data controller. However, the cited provision includes the precondition that personal data processing that aims at the protection of the rights and legally protected interests of the controller may not be in conflict with the right of the data subject to protection of his/her private and personal life. The Office is of the opinion in the long term that publication of the personal data of those persons who fail to fulfil their contractual obligations (debtors) without their consent constitutes inadmissible infringement on the privacy of these persons, because disclosure of this data, which was obtained under a private-law relationship, could harm the good reputation of the affected person in a number of other relationships, both under private law and under public law. This is a form of pressure that also violates Art. 10 (1) to (3) of the Charter of Fundamental Rights and Freedoms, according to which everyone is entitled to protection of his or her human

dignity, personal integrity, good reputation, and his or her name, everyone is entitled to protection against unauthorized interference with his or her personal and family life, and everyone is entitled to protection against unauthorized gathering, publication or other misuse of his or her personal data.

In conclusion, it can be stated that, in all the above-described situations, with which the Office dealt in administrative proceedings in 2009, the Office ruled on violation of the Personal Data Protection Act and imposed a penalty.

SECURING PERSONAL DATA

In 2009, similar to the previous years, the Office again dealt with a number of cases where personal data were disclosed to unauthorized persons because of inadequate security measures taken by the controller or processor. The duty of the controller (processor) of personal data to adopt security measures aimed to prevent unauthorized or accidental access to personal data, their change, destruction or loss, or their unauthorized processing or misuse, is expressed in Article 13 of the Personal Data Protection Act.

In 2009, the Office thus dealt with, e.g. the loss of applications, serving for registration of insured persons with an insurance company, in a bar; theft of documents (by a hacker) containing the personal data of the payers of premiums for health insurance from a home computer of an employee of the health insurance company; documents originating in the activities of the Police of the Czech Republic found in a waste container near the police station; "destruction" of documents with personal data in an unused chimney and the subsequent dissemination of partly burnt documents into the surrounding area; documents found on the street; provision of a copy of a medical report to the manufacturer of food for children; and disclosure (by an unknown person) of a recording of a telephone conversation between a client and the operator of an internet service provider.

In relation to these cases, the Office repeatedly held that the situation itself, when personal data leave the "sphere of control" of the controller, and are thus found on the street or on some other public premises, stolen by an unknown thief, etc., means that the controller has failed to adopt and implement adequate security measures and thus breached the duty imposed on him by Article 13 of the Personal Data Protection Act; this conclusion is not dependent on the degree of fault on the part of the controller, since all these cases involved administrative offences committed by legal entities or natural persons in their business activity. Under these circumstances, the controller is liable for an administrative offence based on strict liability.

In order to alleviate the harshness of such liability, the Act stipulates that the liability for an administrative offence expires if the controller proves that he exerted all the efforts that could be required to prevent the breach of the legal duty; this represents "liberation" from liability for an administrative offence (cf. Article 46 (1) of the Personal Data Protection Act). In all the above cases, the Office noted, with respect to fulfilment of the mentioned condition, that mere adoption of internal regulations, guidelines, security measures in the form of (physical) safeguarding of premises, measures in the area of securing IT systems, etc. cannot be deemed to be exerting all efforts, but rather that these measures must be consistently applied in practice and their adoption and compliance with these measures need to be required and checked. In this relation, it was further ruled that, where the controller is unable to determine or reconstruct the manner of unauthorized access to personal data (i.e. where it cannot be ascertained which of the employees took them out of the premises, who left them on the street, how they could be stolen from the office, etc.), he cannot be relieved from his liability under any circumstances.

In its control and, subsequently, administrative practice, the Office also dealt with the issue of securing the automated tax administration system (ADIS). It was found in this respect that the administrator of this system, i.e. the Ministry of Finance, failed to make electronic records that would make it possible to determine and verify when, by whom and for what reason the personal data were

recorded or otherwise processed (i.e. record and reading logs), which is at variance with the duty pursuant to Article 13 (4) (c) of the Personal Data Protection Act. Given the scope of the personal data processed within the ADIS system and the risks associated with such an inconsistent approach to their protection, the Office imposed the highest fine for this administrative offence of those imposed for breach of security measures pursuant to Article 13 of the Personal Data Protection Act in 2009 (in the amount of CZK 350,000). In this connection, it should be emphasized that, precisely for the reason of risks connected with personal data processing in information systems, the Personal Data Protection Act stipulates, in Article 13 (4), special duties imposed on the administrators of these systems, which must be fulfilled without any reservations.

PUBLISHING PERSONAL DATA IN THE MEDIA

In 2009, the Office also dealt with the issue of publishing personal data in the media. This is undoubtedly one of those problematic areas where two absolutely different interests mutually collide – on the one hand, the justified requirement of the affected persons for the protection of privacy and, on the other hand, no less important freedom of dissemination of information. Given the fact that the Personal DataProtection Act is (in addition to other legal regulations) intended particularly for protection of individuals against unauthorized interference with their privacy by means of processing personal data, the Office is of the opinion that it is absolutely justified to apply the requirements of the Act also in this sphere, even if subject to certain limits. These limits are established by the requirement expressed in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter the "Directive"), which was transposed to the Czech legislation by the Personal Data Protection Act and according to which certain derogations and exemptions from the general regulation of personal data protection should be introduced in the area of journalism. Although this requirement was not fully implemented in the Personal Data Protection Act or in any other relevant legal regulation, in the light of the case-law of the European Court of Justice, the Personal Data Protection Act needs to be applied in the spirit of the requirements of the Directive. Another limitation for application of the Personal Data Protection Act to journalistic activities consists in the principles of interpretation of constitutional rules defined by the Constitutional Court, which has ruled that none of the fundamental rights may be assigned higher importance. Specifically, the Constitutional Court ruled that the fundamental right pursuant to Art. 17 of the Charter of Fundamental Rights and Freedoms (the right to freedom of expression and to information; hereinafter the "Charter") is, in principle, equal to the fundamental right stipulated in Art. 10 of the Charter (the right to protection of personal rights, including personal data).

Given the above-described background, the Office considers it justified to apply entrusted competence in the area of journalism only in extreme cases where measures under public law are substantiated (within the meaning of the *ultima* ratio principle in relation to criminal punishment expressed by the Constitutional Court). Evaluation of the gravity of a given case and justification of the Office's intervention is based particularly on the position of the person to whom the published data relate, the character of the published information and the sense and purpose of publication of the personal data. It is necessary to distinguish information concerning the privacy of, e.g., politicians or "celebrities" from information on "normal" people; a stricter approach should also be taken in terms of publishing personal data concerning children or youth, or persons who are unable to sufficiently defend themselves for some other reason. Analogously, it is necessary to respect the requirement for increased protection of sensitive data as defined in Article 4 (b) of the Personal Data Protection Act. Last but not least, the Office considers it important whether the publication of certain information is to serve purely to increase the "attractiveness" of the message, or whether the processing (publication) of personal data in the given case pursues an actual public interest.

Based on the above-described background and criteria, the Office applied the requirements of the Personal Data Protection Act, e.g. in a situation where sensitive data on the state of health was published in connection with providing information on search for a missing minor person. In a situation where the Police of the Czech Republic evaluate the given case in that the search for a missing person does not require statement of detailed information on the state of health, it is not admissible from the view of the Personal Data Protection Act for other entities (providing news) to search for the details on the state of health in other sources and publish these details together with other sensitive information on the life of the missing person on the grounds of allegedly pursuing a public interest consisting in the right of the public to information. In a similar situation, it is clear that the provision of information supplemented by details on the state of health (or other information, e.g. on sexual behaviour) substantially infringes on the rights of the missing person, while non-publication of these data would neither endanger nor infringe values of the same importance (particularly the freedom of expression). Thus, the Office considers that the mentioned circumstances are absolutely sufficient to infer liability for an administrative offence in processing personal data in the area of journalism.

The Office provided a more detailed opinion in this respect in its statement No. 5/2009 – Publishing personal data in the media.

REGISTRATION

From the summary registration activity that the Office is obliged to pursue according to the Personal Data Protection Act, we can select several illustrative examples that characterize, to a certain degree, a trend persisting in personal data processing in 2009.

In connection with the rapid development of information technology, the Office repeatedly dealt with cases related to the functioning of new technologies intended to secure access to restricted work-places which also allow for processing personal data. This is true, e.g. of the "3D-biophotopotrait" technology. It was inferred from the provided information that the binary chain from which the image of the face cannot be reproduced is not biometric data; nevertheless, it might constitute personal data.

A company showed interest in operating an internet portal where the visitors would obtain, after entering the date of birth, their probable personal profile on the basis of the Chinese horoscope cycles. The company intended to record the other entered data (sex, abilities, skills, characteristics, feelings, state of health, height and weight, opinions and hobbies) in the database with the aim to extend the sample that it could use to further examine and elaborate the principles of the personal profile based on the date of birth. In case of unregistered users, these data would be anonymous only in those cases where information on the IP address, which is a personal data, is not collected and processed. For registered users, where the company would further collect other personal data, such as the e-mail address and name, this would involve processing of sensitive data, which is subject to all the duties following from the Personal Data Protection Act.

Another novelty related to personal data processing was represented by a project where data were processed with the aim of creating an internet browser that would allow the registered users (e.g. personnel agencies) to seek websites with the relevant information on the education and practice of professionals in the given field. The browser operated on the same principle as usual browsers (Google, Seznam): the computer program continuously browsed websites and recorded each relevant word with a very short sample of the given site and indexed this in its own database. The inquiry made by the user was compared with the database of relevant words and extracts from the websites where the words occurred. Unlike usual browsers, which index the entire contents of the web, this project was to index only those sites that were important from the viewpoint of the expertise and practice in the given field.

The registration department very often encountered, in its activities, the issue of monitoring (recording) telephone conversations with clients, business partners, etc., mostly in order to increase the quality of services provided by a help line, to resolve disputes concerning the contents of the calls, to evaluate the quality of information provided by employees, and to provide for training of employees. Where telephone calls with clients, business partners, etc. are recorded, this constitutes personal data processing pursuant to the Personal Data Protection Act provided that the caller is identified, e.g. in the database of clients with verification of the identity, for example on the basis of a password, PIN, etc. and the entire contents of the call are thus personal data.

The above-mentioned examples document a general trend where the Office is forced to assess much more complex and sophisticated types of personal data processing (projects) which relate to the development of new information and communication technology, including processing on the Internet. Another frequent type of reported cases of processing, similar to the previous year, consisted in processing through video surveillance systems, and also processing of data in trade, including e-shops, marketing, advertising and consumer competitions.

TRANSFER OF PERSONAL DATA ABROAD

A vast majority of applications pursuant to Article 27 (4) of the Personal Data Protection Act, which are dealt with by the Office within its competence, are concerned with transfers of personal data to the United States of America. Most often, the recipients of these data are companies with which the applicants are interconnected through capital, and also business partners of the applicants. Given this fact, most frequently the declared purposes of processing and transfer of data were those that directly related to the personnel and salary policies and to business and production activities (e.g. administration of a database of job vacancies; keeping records of job applicants; planning professional development of employees; setting and evaluating working goals; planning business trips; optimization of production procedures, etc.) Consequently, these cases involve transfers of personal data of employees or job applicants to parent companies abroad, particularly to the United States of America. In these cases, given the fact that such processing can be qualified as repeated, collective or structural, the Office recommends that the controllers utilize a special legal framework for transfers, i.e. a contract that will include standard contractual clauses, binding corporate rules or, in case of transfers to the U.S.A., the "Safe Harbor" instrument.

Unfortunately, in these cases, the controllers often rely on consent granted by the employees as the legal ground for the transfer. While this is certainly possible, such transfers also have certain drawbacks, which are often not sufficiently acknowledged by the controllers. The aspects of transferring employee data abroad are not limited only by the conditions stipulated in the Personal Data Protection Act. These transfers must be viewed not only in terms of application of the Act, but also from the viewpoint of other legal regulations, particularly regulations providing for employment relations. The relevant consent of the data subject must fulfil the requirements stipulated in Article 4 (n) of the Personal Data Protection Act, according to which such consent must be a free, explicit and conscious manifestation of will of the data subject. For example, free consent in an employment relationship means that, given the subordinate relationship between the employee and the employer, the employee must have a real opportunity to deny it, without incurring any harm, and also the possibility of subsequently revoking the consent. Informed consent requires that the data subject be properly informed in advance of the specific circumstances of the transfer (its purpose, scope of transferred personal data, recipient(s), etc.); this duty to provide information is also embodied in Article 5 (4) and Article 11 of the Personal Data Protection Act. Information provided to data subjects must also include information on the special risk following from the fact that their data will be transferred to a country that does not provide for an adequate level of protection of personal data. Consent to a

transfer of personal data to third countries should also be separate from the consent or confirmation that the data subject has been acquainted with the conditions of the actual personal data processing.

An increased number of transfers taking place on the basis of the "Safe Harbor" principles was recorded in 2009.

LEGISLATIVE ACTIVITIES

The legislative developments brought two new areas of competence to the Office in 2009:

From April 1, when Act No. 52/2009 Coll. added **definitions of new offences** to the Personal Data Protection Act, the Office has been obliged to prosecute conduct consisting in breach of the prohibition of publishing personal data stipulated by other legal regulations. This amendment accompanied the "Muzzle Act", a change in the Code of Criminal Procedure which responded to repeated publication of large quantities of personal data coming from the criminal proceedings mostly in tabloids, also in relation to minor persons. The Office considered it positive that the amendment pointed out particularly the dangers associated with unrestricted publication and bulk disclosure of personal data (including publication in the media and on the Internet). Unfortunately, within the public debate accompanying this change in the criminal procedure, or rather a critical campaign in most media concentrating on the alleged suppression of the freedom of speech, the original objective of the amendment was often neglected: to protect the privacy of persons injured in crimes (the victims).

Act No. 111/2009 Coll., on basic registers, imposed on the Office, within the newly created eGovernment system, the duty to establish "source" and "agenda" identifiers of natural persons and to provide for transfer of the agenda identifiers of natural persons within the individual electronic agendas. The new identifiers should, amongst other things, reduce the risk of unauthorized treatment of citizens´ personal data stored in state registries. The Office accepted the mentioned competence under a precondition that the creation and transfer of identifiers would take place in a manner ensuring maximum security and that the entire process of generating the identifiers would be strictly separated from any actual processing of personal data by the authorities. At the same time, the current supervision by the Office over personal data processing within the existing state registers and the newly proposed basic registers is in no way prejudiced.

A topic that has yet to be completed and that fundamentally affects the Office's competence **consists in the preparation of the new Control Act**. During the expert meetings with the draftsmen of the Act and also within the commentary procedure, the Office requested that the principles of the uniform procedure within supervision (control) performed by the public administration in the Czech Republic be harmonized with the special and comprehensive requirements for supervision in the area of personal data (according to the EU law). In this relation, it proposed simplification of certain official formalities in respect of the procedures preceding commencement of control in a way analogous to the administrative proceedings as stipulated by the Code of Administrative Procedure. From the viewpoint of its competence, the Office perceives the most serious issue, which has yet to be resolved from a systemic viewpoint, in the fact that **the legislation on confidentiality is not uniform**. Certain legal interpretations of the brief regulations on

confidentiality in the individual laws (indeed, there is no general regulation of the conditions of confidentiality and particularly the process of waiving it) would result in blocking part of the information and personal data required for the performed control. It would clearly be absurd if the controlled public institution itself factually determined the scope of information necessary for control in terms of such interpretations; however, the Office has already encountered this "obstruction" in a control performed in the area of tax administration.

In respect of the provision of comments on legal regulations, in 2009, the Office most frequently encountered fundamental **shortcomings in the area of changes in automated and centralized processing of data within databases kept by the public administration**. The draftsmen of new legislation usually describe and evaluate the intended personal data processing only in formal terms. It would appear that, in numerous cases, personal data protection is still perceived as a redundancy or burden, rather than an advantage, e.g., in terms of the security of public administration, its effectiveness or transparency. A more comprehensive approach to the protection of the privacy of citizens is still lacking in many parts, particularly of older information systems of public administration. The contemplated eGovernment system should remedy the mentioned shortcomings and, from the viewpoint of data protection, eliminate risky procedures that are based, e.g. on erroneous, obsolete or duplicately maintained data on citizens. A central database of data from school records kept within the sector of the Ministry of Education constitutes one of the cases where the Office, within commentary procedures related to regulations implementing the Schools Act in 2009, repeatedly stated its concerns in terms of the scope and necessity of collecting data on citizens required by the law.

In early 2009, the Office sent a letter to the Ministry of Foreign Affairs where it pointed out the **inadequate progress of legislative work in the sector of health care in the preparation of databases containing the sensitive data of citizens**. Following negotiations concerned with health-care registers, which were proposed within a package of laws on health-care services in an unchanged obsolete form, not suiting the principles of personal data protection, this problem was also clearly highlighted in respect of the **central register of electronic prescriptions**. This mammoth database, intended as a central storage place for information on all medical prescriptions (however, with the consequence of keeping information on patients, their physicians and pharmacists), was not presented at all within the draft and discussed within the proper legislative procedure; on the contrary, it was approved as one of a number of MP's motion for supplementing the Pharmaceuticals Act.

A control performed by an inspector of the Office revealed variations between the brief legal regulation and the scope of the collected data. When the Ministry of Health subsequently proposed, in late 2009, rapid modification of the legislation, the Office requested that it clarify the purpose of the database and the related tasks of the State Institute for Drug Control, which administers the database, and also justify of the mandatory establishment of a medicament record for each patient, and further requested that the need for the entire system be substantiated and the requirements following from the EU law consistently reflected.

2009 was a year when the general public showed considerable interest in new technologies that could interfere with the privacy of citizens. With respect to **electronic motorway vignettes**, the Office favourably acknowledged the statutory condition of anonymity and transferability of the vignettes – however, the fulfilment of this condition may be assessed only after the relevant regulations implementing the law have been presented. Indeed, the proclaimed requirement for anonymity or transferability of the vignettes need not be entirely feasible, as each thing designated by a number or registered in a certain way which is used by a certain person can be utilized to identify the person. In addition to clarification of the required scope of data connected with the technology, it will be necessary to take due account of the rules for sharing and further processing of data in the relevant information systems.

For **video surveillance systems**, which have been perceived lately by part of the public as monitoring systems, which should be subject to a special regulation, the Office contributed its expertise to the formulation of the requirements for a legal regulation. In the first half of 2010, the Government requested that amendment to the Personal Data Protection Act be drawn up, including specific rules for collection of data through video surveillance systems, as well as their further processing, including the duty to provide information on processing. The Office anticipates a similar procedure in 2010 in respect of the creation of a law providing for **processing of data on human DNA**.

With respect to the recent developments in the EU law, the Office considered it necessary to point out, within the legislative commentary procedure held in 2009, the issue of a more comprehensive approach to consumer and **loan registers**. The Office recommended that attention be paid, not only to shared bank registers that were already regulated by law, but also to non-bank registers intended for sharing data on certain clients (debtors) with low creditworthiness. These databases are operated in the Czech Republic on the basis of the consent of the affected persons, rather than within statutory authorization.

FOREIGN RELATIONS AND INTERNATIONAL COOPERATION

The international legislation forming the basis for the Office's activities remained practically unchanged in the year of interest. It continues to include two basic directives (95/46/EC and 2002/58/EC), Council of Europe Convention No. 108/1981 adopted by the European Union for certain instruments of the 3rd pillar and a number of legal acts with a strictly defined area of application, such as numerous decisions of the Commission acknowledging the adequacy of personal data protection in certain third countries outside the EU and EEA or in the use of specific (e.g. standard contractual) guarantees.

The permanent priority attached to cooperation with the EU bodies and partner authorities in the EU Member States within foreign relations of the Office was strongly highlighted in the first half of the year by activities related to the Czech Presidency in the EU Council. Three important **activities** were pursued by the Office **within the Presidency**:

(1) The fact that the Czech Republic took over the Presidency from France inspired the Office to invite their French colleagues from the partner authority CNIL – Commission Nationale de l'Informatique et des Libertés, headed by its President, Mr Alex Türk, who is simultaneously the chairman of the Article 29 Data Protection Working Party (WP 29 – see below). The French delegation stayed in Prague from March 3 to 4, 2009; in addition to a working meeting and sharing experience with the experts of the Office, it also visited the Senate of the Parliament of the Czech Republic, where it discussed various issues with the members of the Senate Standing Committee on Privacy Protection and was received by the President of the Senate, Dr Sobotka. The program also included a round table discussion at the French Institute, concerned with the protection of privacy of children against Internet risks, which was also the topic of a joint press release.

(2) The organization of the 19th "Case Handling Workshop" in Prague from March 12 to 13, 2009 was the most demanding event within the Presidency in organizational terms and attracted a lot of international attention. The workshop is a regular working meeting of the chief experts on control activities from independent supervisory bodies, similar to the Office, which takes place alternately in various host countries of the EU. Representatives of analogous authorities from several European countries outside the EU were also invited. The main topics included the relationship between the media and personal data protection, with an attempt to strike a balance between the right to freely seek and disseminate information and the right to privacy. The meeting also dealt, e.g., with the frequent use of video surveillance systems, processing employee data and handling personal data of patients in health care.

(3) In direct relation to the Czech Presidency, the Office convened a meeting of the Council's/Coreper's G.09 working party for personal data protection (Brussels, March 23, 2009). Not every Presidency resolves to organize a meeting of this working party. The Office initiated its convening, co-organized it and participated in its program, although it is not its member, since it cannot

represent the Czech Republic in the Council's working bodies given its independent position. As the main item on the agenda, the representative of the Office presented, with certain critical notes, information on the newly adopted EU legal regulation – the Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. While this document, which was adopted after years of negotiations, is a step in the right direction with the aim to unify the aspects of personal data protection within the 3rd pillar, it failed to fulfil the original expectations in a number of ways. The Office also prepared a background document for a presentation made by the representative of the Czech Republic in G.09 from the Permanent Representation of the Czech Republic in the EU in relation to the highly controversial topic of preparation of a proposal for a Council Framework Decision on the use of the Passenger Name Record (PNR) for law enforcement purposes.

The main platform for sharing experience, refining the practice and unifying the approaches of the data protection authorities of the EU Member States is provided by the **Article 29 Data Protection Working Party**.

Participation of the Office in European Supervisory Authorities

Within its foreign activities, the representatives of the Office also participate in meetings of the joint supervisory authorities established for the purpose of supervising shared European information systems, namely:

- the Joint Supervisory Authority – JSA Schengen;
- the Joint Supervisory Authority – JSA Customs;
- the EURODAC Supervision Coordination Group;
- the Joint Supervisory Body - JSB Europol.

From the view of the Office, participation in the activities of these authorities provides an opportunity to obtain further experience in the area of control of extensive information systems, and particularly the possibility of influencing the contemplated joint approaches and methodologies, and also new European legislation regulating shared databases (with constant pressure on extending the scope of the processed data, as well as the scope of entities to which they are disclosed).

In addition to control of data processing within the Schengen Information System and participation in JSA Schengen, the representatives of the Office also participate in regular evaluation of the level of personal data protection in other Schengen countries. In 2009, the evaluation was concerned with as many as five Member States (Belgium, Netherlands, Luxembourg, Germany and France) and two accession countries (Bulgaria and Romania), where, in view of the Czech Presidency in the EU Council in the first half of 2009, the representatives of the Office were entrusted with the demanding role of leading experts in the framework of these evaluation missions. The Office was properly represented at all four plenary meetings of JSB Europol and two meetings of its appeals committee. Furthermore, a representative of the Office, who is also involved in three working subgroups, acted as the coordinator of the control team which performed regular control at the Europol headquarters in March 2009.

The Office also participated in the work of the Working Party on Police and Justice.

The 30th International Conference of Data Protection and Privacy Commissioners in Strasbourg in 2008 approved the mandate for a working party that should attempt to formulate "global standards" of personal data protection. The main work coordinated by the Spanish Data Protection Agency took place in 2009 and the results of the efforts, a contribution to which was also made by the representatives of the Office in the form of written comments and participation in two working meetings (in Barcelona in January and in Bilbao in June 2009), could be presented at the 31st International Conference in Madrid in November 2009. In addition to the EU and its bodies, an important platform for multilateral cooperation is also provided by the **Council of Europe and the Organization for Economic Cooperation and Development (OECD)**.

Within the **Council of Europe**, the Office continued to actively participate in the seven-member bureau of the Data Protection Committee established pursuant to Convention No. 108 (T-PD).

For a number of years, in cooperation with the former Ministry of Informatics and later the relevant section of the Ministry of Interior, the Office has participated in the activities of **WPISP – the Working Party on Information Security and Privacy in the ICCP Committee within the OECD Secretariat**.

Interest in workshops and working meetings, which are mostly organized in Prague and where the Office shares its experience in the areas of legislation and practice, has recently rapidly increased in the framework of bilateral cooperation with the newly established European and non-European bodies in the sphere of activities similar to the competence of the Office. The participants are interested particularly in the organizational structure of the Office, its strong competence and mechanisms of supervisory activities, including practical findings from controls and the related administrative proceedings, the traditionally successful public relations and international cooperation. In 2009, the Office thus organized two workshops for the Data Protection Agency of Bosnia and Herzegovina (in Sarajevo and Prague), twice invited to Prague a group of colleagues from the Albanian Data Protection Commission which is currently being formed, shared its experience with a four-member delegation of the Chinese Ministry of Industry and Information Technologies during its study trip around the EU and also met law students from Georgia in Prague.

Participation of the representatives of the Office in international conferences, seminars, workshops, etc.

The **European Privacy and Data Protection Commissioners' conference** (Edinburgh, April 23 to 24, 2009) and the **31st International Conference of Data Protection and Privacy Commissioners** (Madrid, November 4 to 6, 2009).

THE OFFICE, MEDIA AND MEANS OF COMMUNICATION

In 2009, the Office continued the tradition of organizing balancing press conferences; however, communication with the media was focused mainly on everyday service and provision of topical information on the website.

The number of releases published in connection with personal data protection based on the press conferences corresponded to the previous year (30 to 60 outputs within three days following a press conference). In annexes to the press releases, the Office consistently provides information on controls completed through administrative proceedings.

Contact with media

It can be stated in general that general knowledge of the Personal Data Protection Act is constantly increasing. This conclusion is based particularly on the everyday service provided to journalists, who raise much more qualified and accurately formulated questions than in the previous years, and point out cases which are mostly really relevant from the viewpoint of violation of the law. This also corresponds to the experience with complaints received by the Office.

A similar conclusion can be drawn on the basis of the topics covered in direct presentations in the media, which are requested from the President of the Office, professional employees and the spokesperson.

The Office usually publishes the media outputs on its website. This helps the public to observe the continuity in the Office's opinions and provides journalists with instant answers to the questions raised.

However, it remains true that it needs to be repeatedly explained that the Office is not authorized to initiate legislative work and that, in the resulting legislative steps, it is obliged to respect the will of the legislature, although it puts forth its qualified comments on legal regulations in the field of personal data protection and respect for privacy with regard to domestic and European legislation and case-law. It is also true that the "impatience" of the media and individuals often prevents acceptance of facts with understanding and a sense for reality.

Dissemination of knowledge on personal data protection

In connection with the Personal Data Protection Day in 2009 and in relation to the fact that, in the first half of the year, the Czech Republic was presiding over the European Union, the President of the Office invited his French peer to a meeting in Prague. Public discussion concerning the current topics of personal data protection was organized in cooperation with the French Institute on the basis of this meeting and with participation of the President of the French Commission Nationale de l' Informatique et des Libertés (CNIL), senator Alex Türk and his company. Also in cooperation with the French Institute, the Office organized a film screening. French document "Total contrôle" directed

by Etienne Labroue and a legendary Czech movie by Vlastimil Venclík, "Nezvaný host" (*"Uninvited guest"*) were shown during an evening entitled "Informatics and Freedom". The Office noted greater participation and a qualitative shift in the competition for children and youth "This is my privacy! Don't look, don't poke about!". The awards for the winners were presented traditionally within the Zlín International Festival of Films for Children and Youth, with the participation of the Chairman of the Senate's Standing Committee on Privacy Protection, Senator Jana Juřenčáková, and Senator Václav Homolka. The competition works of the children were exhibited under the auspices of Senator Juřenčáková on the occasion of the beginning of the new school year in the anteroom of the Meeting Hall of the Senate.

The exhibition of children's works was also a welcomed supplement to the professional conference organized by International Data Group, a.s. (IDG). Children's works also attracted the interest of our foreign colleagues: A small exhibition was held in Cyprus and one of the awarded pictures was published together with information on the competition by a journal issued by the personal data protection authority of the Australian state of Victoria.

2009 was the third year when the Office organized a program of ongoing education of pedagogical workers concerned with personal data protection in education within a three-year accreditation by the Ministry of Education, Youth and Sports. Some 200 teachers participated in a workshop in which the Office provided for the relevant expertise; based on tests, which provided the Office with a feedback and information on comprehension of the subject-matter, the participants in the workshops obtained certificates. The workshop attracted sincere interest.

The Office also considered it important to meet with the generation of seniors (in cooperation with the Third Faculty of Medicine of Charles University), to whom it is necessary to consistently explain the sense of personal data protection, as well as raise their awareness of the fact that protection of privacy is their right.

Lectures provided by employees of the Office (the Office's lawyers provided a total of 258 hours of lectures last year) and meetings of the President, inspectors and management of the Office with the Senate's Standing Committee on Privacy Protection are also undoubtedly beneficial. A workshop concerning the issue of DNA profiles, which was initiated on the basis of the Office's control findings, must be unambiguously considered successful. Under the auspices of the Vice-President of the Senate of the Czech Republic, Dr Liška, it was organized by Senator Jana Juřenčáková and the President of the Office in the autumn of 2009. The workshop raised a number of issues that require a precise legislative basis.

Library and publications of the Office

The library continues to serve as a useful source of professional information for the Office's employees; however, at individual request, it is also open to the professional public. It is used by students for their seminar works and theses concerning personal data protection. In 2009, the library provided its sources to seven students and newly obtained two theses and one seminar work.

In its 4 volumes, the Journal of the Office published important foreign documents on personal data protection as well as fundamental statements of the Office. Four volumes of the Information Bulletin were, as usual, published in 2009.

NEW AREA OF COMPETENCE OF THE OFFICE – ORG INFORMATION SYSTEM

Act No. 111/2009 Coll., on basic registers, provides for the establishment of basic registers, including the development of an information system for the creation of agenda identifiers of natural persons (the ORG information system within the system of basic registers of the public administration – ORG), with effect from July 1, 2010. This gives rise to a new area of competence of the Personal Data Protection Act.

The entire concept of the system of basic registers (BR) is grounded in several principles, which aim mainly at protection of data against misuse, which is precisely the objective of the ORG project. The first principle lies in the use of a system of meaningless identifiers of natural persons. Each natural person will be assigned a "source identifier", from which further, "agenda" identifiers of natural persons will be derived for each agenda where the given person is involved. Given the fact that a certain person will be designated by a different identifier within each agenda, it will be possible to prevent unauthorized sharing of data amongst the individual agendas. Another security measure consists in strict division of roles between various authorities. Thus, in practice, one authority will administer the register as such, while another authority will provide for the operation of the information system of the basic registers; last but not least, a special role will be played by the Office for Personal Data Protection, which will generate the identifiers of natural persons for the individual agendas and provide for their mutual transfers based on authorized requirements. The concept also includes a central system of administration of the roles for access to data, which will ensure that only the officer authorized to this end by the law will be able to access each reference detail in the individual basic registers. Of course, all cases of access to the reference data will be recorded and it will thus be possible to check them retroactively at any time.

Act No. 111/2009 Coll., on basic registers, introduces the following functional blocks of the system of basic registers:

- the basic register of population (hereinafter ROB);
- the basic register of legal entities, natural persons operating a business and governmental authorities (hereinafter ROS);
- the basic register of territorial identification, addresses and real estate (hereinafter RUIAN);
- the basic register of agendas of public authorities and certain rights and duties (hereinafter RPP);
- the information system of basic registers (hereinafter ISZR);
- the ORG information system (hereinafter ORG).

ORG information system in the system of basic registers

The ORG information system is an independent functional block of the system of basic registers, which will provide for processes concerning identifiers of natural persons. This includes, in particular, the following processes:

- It creates the source identifiers of natural persons and agenda identifiers of natural persons and keeps a list thereof.
- It provides for transfers of agenda identifiers of natural persons in one agenda to agenda identifiers of those natural persons in another agenda, based on a lawful requirement.

Identifiers of natural persons include:

- Agenda identifier of a natural person (hereinafter AIFO) is a non-public identifier, which is unambiguously assigned to the record on a natural person; it is inferred from the source identifier of the natural person and the code of the given agenda, and is used exclusively for unambiguous determination of the natural person for the purposes of the agenda for which it was assigned. The source identifier of the natural person or personal or other data on the natural person to whom it was assigned cannot be derived from the agenda identifier.
- Source identifier of a natural person (hereinafter ZIFO) – is a non-public identifier that is kept and used exclusively in the ORG information system for the creation of agenda identifiers of natural persons for the individual agendas. Personal or other data on the natural person to whom it was assigned cannot be derived from the source identifier.

  A natural person can be identified in a single agenda only through the single agenda identifier of the natural person.

Division of the project to individual phases will allow for gradual implementation of ORG depending on the development of the other parts of the Information System of Basic Registers (ISZR). Given the fact that the generation of ZIFO and AIFO is a key functionality, which must be available already at the beginning of implementation of the BR, the schedule is proposed so that this basic functionality with limited performance is available during 2010.

PERSONNEL OF THE OFFICE

96 positions were approved for the Office in the state budget for 2009, of which one position was intended for the performance of tasks following from the Czech Presidency of the EU Council in 2009. This position was cancelled on September 30, 2009.

As of January 1, 2009, the Office had 93 employees, of which 90 positions were occupied and 3 employees had an off-record status.

As of December 31, 2009, the Office had 95 employees (of which 3 employees had an off-record status).

11 new employees joined the Office and 9 terminated their employment during the year.

The average recalculated number of employees on-record in 2009 equalled 90.807.

2/3 of the Office staff are university graduates and approx. 1/3 of employees have completed secondary or secondary vocational education. The Office allows its employees to improve their qualifications and also provides for their extension and increase; it also provides language courses in the English, French and German languages.

ECONOMIC MANAGEMENT OF THE OFFICE

The budget of the Office was approved by Act No. 475/2008 Coll., on the state budget of the Czech Republic for 2009.

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

	in CZK thousand
Summary indicators	
Total income	3 104.40
Total expenditures	91 816.19
Specific indicators – income	
Total non-tax and capital income and accepted transfers	3 104.40
Specific indicators – expenditures	
Expenditures for the performance of tasks of the Office	91 816.19
of which: expenditures related to the Czech Presidency in the EU Council	1 162.25
other expenditures for the performance of tasks of the Office	90 653.94
Cross-cutting expenditure indicators	
Salaries of employees and other payments for performed work	41 705.00
Mandatory insurance premiums paid by the employer *)	14 181.00
Contribution to the Cultural and Social Needs Fund	789.44
Salaries of employees within an employment relationship	30 493.00
Salaries of employees derived from salaries of constitutional officials	8 972.00

*) premiums for social security and the contribution to the State employment policy and premiums for the public health insurance.

PROVISION OF INFORMATION PURSUANT TO THE ACT ON FREE ACCESS TO INFORMATION

In 2009, the Office received a total of eleven requests for the provision of information pursuant to Act No. 106/1999 Coll., on free access to information, as amended. Compared to the previous year, when the Office received six requests, this is almost a two-fold increase.

In two cases, the request for information was rejected (in both these cases, the applicants appealed against this decision to the President of the Office); in the remaining cases, the requests were satisfied. Furthermore, in accordance with the duty imposed on the Office by Article 5 (2) of the Act on Free Access to Information, the contents of the provided information were published on the Office's website.

Seven requests for the provision of information were concerned with specific proceedings, where the applicant inquired about the manner of resolving his instigation or the result of some other proceedings, or whether the Office actually performed a control or held proceedings in the given case. One request related to the personnel of the Office, one applicant requested that published statements of the Office be sent to him, in one request, the applicant asked what personal data and for what purpose the Office generally processed, and one request was concerned with the procedure of the Office in the provision of information.

The number of requests for consultations to which the Office is obliged to reply pursuant to Article 29 (h) of the Personal Data Protection Act and that were incorrectly designated by the applicant as a request for information slightly decreased; nevertheless, some requests were again incorrectly designated.

ANNUAL REPORT SUMMARY 2009

ANNUAL REPORT SUMMARY 2009
The Office for Personal Data Protection
Pplk. Sochora 27, 170 00 Praha 7, CZ
E-mail: posta@uoou.cz
Web: www.uoou.cz

In February 2010, the annual report was published on the basis of duty imposed by articles 29 (d) and 36 of the Act no. 101/2000 Coll., on the protection of personal data and of amendment to some acts.

Editor: Hana Štěpánková, tel.: + 420 234 665 286
Editorial revision: Nina Táborská
Graphic layout: Eva Lufferová