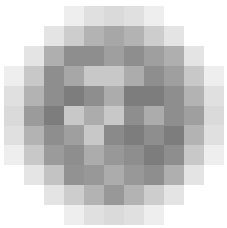
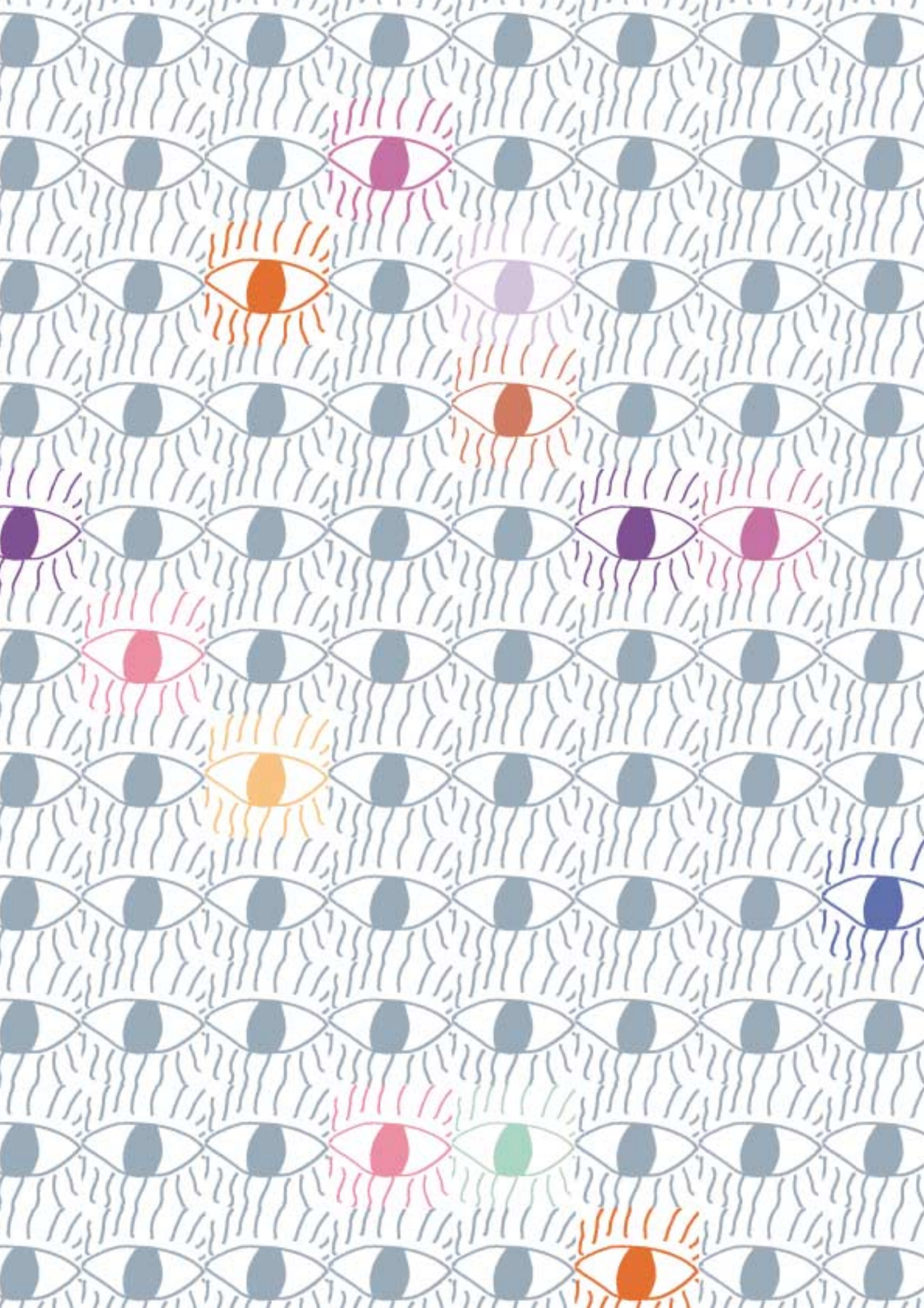


the office
for personal
data protection

Winner of the
Prize to Data
Protection Best
Practices in
European Public
Services 2007

ANNUAL REPORT 2007

SUMMARY



Year 2007 from the Viewpoint of the President of the Office

Looking back over the past year, I recall events that took place in relation to personal data protection and remind myself that, at the beginning of the 21st century, we are witnessing a strengthening of democracy, while human freedom appears to have become a less important aspect. It would seem that collective issues, such as protection against global climate change or joint fight against terrorism, have assumed greater importance than personal freedom. Measures are being gradually enforced without consideration of the risks, difficulties and costs that could be incurred by individual persons whose freedom, such as the right to privacy, is thus being restricted.

We can witness a shift in the pendulum towards collective security, as well as comfort, to the detriment of the right to privacy. This is all happening with the uninformed consent of a majority of the population. It is clear that even a number of responsible officials do not realize that invasive intervention in the privacy of citizens could ultimately be a means of breaching the safety of us all.

The Czech Office for Personal Data Protection is one of institutions that strive to draw attention to this phenomenon. Thus, we are an office that deals not only with specific complaints and instigations, with subsequent imposition of penalties – although this is being performed as our statutory duty – but we also perceive ourselves as a preventative authority that attempts to draw attention to problems, not only within legislative activities, but also in public promotion of personal data protection.

Indeed, this could be the reason why we received the Prize for Data Protection Best Practices for 2007 awarded by the Data Protection Authority in Madrid. We simply feel that we must draw attention to the risks related to mass processing of personal data, accompanying the rapid development of information technology. We closely monitor these trends both in this country and abroad, and we speak about this phenomenon whenever we are able to communicate with the citizens of this country – we provide consultancy, give lectures, organize workshops and provide time to the media. We also do not try to save time in our internal professional discussions. Indeed, those who protect personal data are also constantly facing new issues following particularly from the aforementioned rapid development of new technologies. While these technologies ultimately provide people with greater comfort, they also pose greater threats to private, and even the most intimate, lives of individuals; this is why it is so important to search for balanced options for their use, following from the laws. Nevertheless, I must note with satisfaction that our contacts with the legislator and, specifically, with the Standing Commission on Privacy Protection of the Senate of the Parliament of the Czech Republic became more intensive in 2007 and I attach great expectations to this fact from the viewpoint of future positive steps aimed at protecting the privacy and freedom of each of us.

Naturally, I would welcome it if the detailed specification of issues in the area of personal data protection, as indicated in the overview pertaining to the last year, which is presented in the first chapter of this annual report, also became an inspiration for our legislator and executive authorities. This overview is based on the highly practical and specific findings of inspectors of the Office; however, it also provides reflections on the current obstacles to securing the right to the private and family life of each citizen and the dangers affecting our privacy. In my opinion, we

thus not only fulfill the duty of a supervisory authority, which the Office undoubtedly continues to be, but also provide another positive option for development of an institution that will provide a real service for the public.

For me, it is a challenge and honor to be "part of this". I am very well acquainted with the trends in this subject in our country. I was the first to speak about this topic in the Czech Republic at an international conference organized in 1997 by the State Information System Authority, of which I was the chairman. I can well recall the atmosphere in society, in the Chamber of Deputies and in the Senate. There had never been any demand for protection of personal data. And it was no wonder. A lot of information seemed to come from a sci-fi world. Indeed, at that time, mobile telephones were just becoming part of our lives. However, it must be seen that, since then, with the development of information technology, a great many people have changed their attitudes. A number of questions and also specific problems have arisen. The Czech Personal Data Protection Act was adopted in 2000, together with the establishment of the Czech supervisory authority – the Office, which was conceived as one of a few authorities protecting citizens in an area where citizens can hardly manage without assistance and, in a number of cases, are not even aware of any danger.

At the present time, the Czech Office for Personal Data Protection is well established in the system of public administration. It is characterized by its dynamic nature, both in its organizational structure and in its competence and communication strategy. Its attempt to keep pace with the developing subject of personal data protection can also be documented by the amendments to the Personal Data Protection Act that have been adopted over the 7 years of its existence, as well as by the series of reorganizations that were initiated by changes in the competence of the Office (most recently, e.g., organizational changes caused by accession of the Czech Republic to the Schengen area).

However, I am also glad that we have been and continue to be able to discuss these aspects with the public and that our citizens are becoming increasingly aware of the risks related to a careless attitude towards their property – personal data – which is reflected in an increasing number of questions, complaints and registrations.

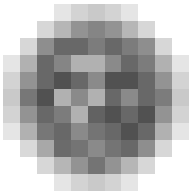
I am also very delighted that we have been able to share some of our experience within the twinning project that we implemented in Bosnia and Herzegovina.

What is more, I am also very favorably inclined towards international cooperation because, as a person who has spent part of his life working as a mathematical expert in the area of information technology, I am well aware that no State borders can automatically protect personal data.

However, I primarily believe that, together with the legislator, we can take a great many useful steps in the area of personal data protection to protect the privacy and freedom of people.

Igor Němec
President

Contents



Activities of Inspectors

I. Findings obtained by inspectors in control activities

GOVERNMENTAL AUTHORITIES

An extensive control was performed in the area of activities of a central governmental authority whose competence includes selection and preparation of judicial candidates and other persons applying for the office of judge. It was ascertained that this body held certificates and affirmations in its personnel documentation kept pursuant to the Lustration Act with respect to persons born after December 1, 1971; in the proposals for appointment of judges, it presented information on the family status, the number of children and the employer of the spouse of an applicant for the office of judge; it also specified the nationality of the applicants and obtained from them affirmations on their previous and current membership in political parties and movements. The mentioned authority thus collected redundant information on applicants for the office of judge, including sensitive data, without having the consent of the affected persons in this respect and without having provided them with the information stipulated by the Act. It is important that the mentioned control findings were obtained in relation to the practice of a central authority, which performs administration in the field of justice.

The performed control activities show that it continues to be necessary to pay increased attention to the activities of governmental authorities and bodies of local government. A control performed at an authority of a large city which provides for the election of lay judges to the relevant court by the municipal board indicates that, in the given case, the data controller processed inaccurate data, obtained data on the nationality of the relevant parties, their occupation, numbers of identity cards and telephone numbers, as well as information on criminal proceedings pursued against candidates for the office of lay judge and their relatives, although this is not required by law. As a result of its activities, personal data on privacy of the candidates were published on the website of the city without their consent and the files containing personal data of lay judges were kept by the municipal authority during the entire term of office of these persons. The control also revealed that there was no internal regulation providing for management of supporting materials drawn up for meetings of elected bodies, which contain personal data, by the members of these bodies, particularly after termination of the meeting. The shortcomings found are not the result of a negligent approach of the relevant persons to the fulfillment of their duties, but they rather attest to a lack of understanding of the relevant provisions of the Personal Data Protection Act and the related misconduct, which was often motivated by the effort to satisfy, as far as possible, the justified needs of citizens.

The same was true for the practice of a specialized department of another municipal authority which, in an attempt to accelerate the handling of citizens' requests, sent these requests, including their personal data, to a natural person who was the only one who could decide on the request in accordance with the applicable regulations. Given the fact that the controlled entity was not authorized

to transfer the data (authorization or competence following from special regulations) and acted at variance with the Personal Data Protection Act, the inspectors had to note violation of this Act.

A municipal authority submitted a instigation lodged by citizens to another authority, in order to obtain its opinion, whereby it disclosed personal data of the petitioners without authorization. The affected persons asked the Office as to whether this procedure was in accordance with the Personal Data Protection Act. It was ascertained in the control that personal data on the petitioners were processed at variance with the special regulation and the Personal Data Protection Act. The municipal authority breached the duty of a data controller in dealing with instigations and failed to respect the right of citizens to protection of their private and personal life; a fine was imposed on the authority for this conduct.

POSTAL SERVICES

Repeated controls carried out in the period from 2005 to 2007 documented that a provider of postal services, as an entity processing personal data for other controllers, required, in numerous situations occurring at its branches, that its employees make copies of identity cards of the clients or other documents or deeds of these persons containing personal data. The controlled entity was advised that the mentioned practice was at variance with law. On the basis of the measures that it adopted on the basis of the controls at the end of 2007, it has changed the relevant internal rules requiring the implementation of the mentioned regulations.

Furthermore, a control of the aforementioned entity was initiated on the basis of an instigation sent to the Office in relation to the processing of personal data of citizens – recipients of payments from the social security administration. The complainant provided the Office with payment orders of type B which he found and that contained personal identification of the recipients. The inspectors thus ascertained and verified facts related to the printing and subsequent distribution of type B payment orders by the provider of postal services. The control of processing of personal data of citizens in the printing of payment orders demonstrated breach of the duties stipulated by the Personal Data Protection Act by the provider of postal services. Given its status, the provider of services must provide guarantees of technical and organizational security in personal data processing and adopt measures to prevent any accidental access to these data. On the basis of the results of the control, a fine was imposed on the provider pursuant to the relevant provision of the Personal Data Protection Act.

CONSTRUCTION-SAVINGS COMPANY

A control concerned with the fulfillment of the duties of a data controller and, as appropriate, the processors (construction-savings company and its sales representatives) in the processing of personal data of their clients was initiated on the basis of an instigation submitted by the mayor of a municipality. The instigation indicated a suspicion of unauthorized access to documents containing personal data of the clients of the given construction-savings company after they were found in the district of the municipality. In the relevant case, it had to be stated that the manner of specification of the rights and obligations of the controller allowed, in a certain phase, to process personal data on clients at variance with the Personal Data Protection Act. The data controller failed to adopt adequate measures to prevent unauthorized access to the personal data on clients of the company. During the control, the construction-savings company adopted measures and took steps to prevent any further occurrence of this situation and, thus, unauthorized access to personal data. A fine was imposed on the controlled entity for violation of the Act.

JUDICIAL DISTRAINERS

In 2007, the Office recorded, amongst other things, an increased number of citizens' complaints against judicial distrainers. The complaints related to personal data processing by judicial distrainers did not always prove to be justified. It is clear that ignorance of the relevant legislation, together with the negative consequences for the obliged persons in relation to the distress, cause ambiguities in the relations between distrainers and other parties to distress proceedings, in consequence of which the Office receives complaints against allegedly unlawful procedures of judicial distrainers in personal data processing. Nevertheless, incorrect acts were found to have been made by these persons, who must have university education for the discharge of their office; in consequence, unauthorized persons became acquainted with important personal data about other entities.

In future implementation of the Personal Data Protection Act, it appears to be necessary to continue acquainting both the lay public and, particularly, the professional public with the contents of the Act. The Act is often not respected because the recipients are not acquainted with its contents or, although they are acquainted with it, they do not understand it. Even governmental officials or officers of local governments, who work with numerous personal data, often do not comprehend that these data are specifically protected and the reason for this protection is unclear to them. The mentioned fact can also be explained by persisting inadequate awareness of the possibilities of misuse of personal data.

Unauthorized disclosure of personal data is often also caused by a certain dilemma as regards the balance of personal data protection and the citizens' right to free access to information. Inadequacies in this area can be eliminated only by raising awareness with respect to the contents of the Personal Data Protection Act and the Act on Free Access to Information and clarification of their mutual relation.

This would be facilitated, particularly for minor and small businesses, by drawing up a sample internal regulation that would help these entities fulfill their duties following for them from Article 13 of the Personal Data Protection Act, while contributing to clarification of the often complex wording of this Act and its comprehension by these entities, with subsequent more consistent and better practical implementation of the Act. This regulation should be accompanied by the sample contents of information on personal data processing provided by the obliged entity, sample consent to personal data processing in typical situations and perhaps the wording of the passage concerning personal data processing that is often included in the business terms and conditions that usually form part of business contracts.

In practice, it would also be suitable to clearly determine the consequences of registration pursuant to Article 16 of the Personal Data Protection Act. This is important particularly due to the fact that registration is mostly perceived by the obliged entities as factual consent to implementation of the notified activity.

Based on the results of the control activities, a conclusion can be made as to the most frequent violations of the duties of controllers and processors, as appropriate. There is a continuing tendency amongst data controllers to gather personal data on data subjects to an extent greater than necessary to fulfill the set purpose. The mentioned fact was found not only in the private sector, but also in the public sector.

Controllers (small businesses) often do not correctly comprehend Article 13 (performance of duties by persons in securing personal data) and, consequently, they fail to adequately appreciate the risks in personal data processing and adopt measures to prevent unauthorized or accidental access to this information.

Other, very frequent violations of the duties of data controllers and, as appropriate, data processors include failure to fulfill the information duty pursuant to Article 11 of the Personal Data Protection Act, which imposes on the controller the duty to inform the data subject, within collection of personal data, about the scope and purpose of personal data processing, by whom and in what manner the personal data will be processed and to whom the personal data may be disclosed, unless the data subject is already aware of this information. The controller must inform the data subject on his right to access the personal data, the right to have personal data rectified, as well as other rights. During the control activities performed in 2007, it was ascertained that the mentioned duty was fulfilled only partly, or was not fulfilled at all.

HEALTH CARE

I.

The control performed at the Institute of Health Information and Statistics of the Czech Republic (UZIS), initiated in 2006, was completed last year. The control was concerned with compliance with the Personal Data Protection Act in collection and processing of medical information and keeping national medical registers.

This was a very important control, as UZIS is probably the biggest controller of sensitive data in the Czech Republic from the viewpoint of the scope of the controlled data. In fourteen national medical registers that are part of the National Health Care Information System, UZIS maintains sensitive personal data on a major part of the population of the Czech Republic.

The control was concerned particularly with securing and protecting the maintained personal data against misuse. The control included assessment of the technical design of the relevant information system, technical and organizational measures implemented in the entire process of data processing and conformity of these measures with the relevant standards for security of information systems; the application of internal security regulations and compliance with these regulations in practice was also reviewed.

It was found and stated during the control that, within collection and processing of health-care information and in keeping national medical registers, UZIS duly fulfills all the conditions for protection of personal data as stipulated by law and that the processed personal data are given due and full protection within a scope that can be justifiably expected in processing of sensitive data of such extent.

II.

A control of a non-state health-care facility – a major polyclinic – was completed; this control was performed on the basis of a report that medical cards of the patients of the polyclinic had been found at a waste collection site located several kilometers from the polyclinic. The control revealed medical documents concerning approx. 2000 persons who had indeed been patients of the mentioned health-care facility. The medical documentation was removed from the facility during construction modifications of the building of the polyclinic, when the documentation was not secured against access by unauthorized persons. A positive aspect lay in the fact that the employees of the waste collection site immediately secured the documentation and submitted it to the Police of the Czech Republic, which prevented any potential further misuse.

A fine of CZK 1.75 million was imposed on the polyclinic in the subsequent administrative proceedings. Account was taken particularly of the fact that sensitive data were involved and that the medical documentation was lost due to absolutely

incomprehensible negligence in its handling. The degree of this negligence is striking because it was committed by a health-care facility and health-care professionals, for whom protection of data on patients should always be automatic, even if there were no principles stipulated by law. The fine for the polyclinic was not even higher, particularly because a major part of the documentation found was concerned with already deceased persons.

III.

Given the fact that major health-care facilities having the character of hospitals had already been controlled in the past and that the state of protection of personal data on patients was mostly evaluated as corresponding to the requirements of the Act, the control activities in 2007 concentrated particularly on small non-state health-care facilities – surgeries of private physicians. The reason for this approach also lay in numerous complaints of citizens about inadequate protection of medical documentation in these facilities. The controls revealed that the state of affairs is often unsuitable.

Based on the findings obtained in the performed controls, it can be summarized that very primitive violations of the principles of personal data protection were mostly found, caused by elementary negligence and reliance on the attitude "we have always done this and nothing has happened". The following cases may be stated as typical examples:

■ A private physician providing preventive health care for a company in machine industry on the basis of a contract recommended further professional examination of employees of the company on the basis of their medical check. In order to "accelerate" the procedure, he submitted the recommendations for examination (including diagnoses) to the superior of the employees and asked him to distribute them to the employees, rather than giving them directly to the patients. The patients (employees) of the company were rightly dissatisfied by this procedure. Violation of the Act was noted within the control as the physician failed to adopt measures preventing misuse of sensitive data.

■ The registration of a surgery of a private physician (a non-state health-care facility) was canceled by the regional authority at her own request. The physician had the obligation to submit the medical documentation of her patients to the regional authority. She failed to fulfill this obligation, because the owner of the non-residential premises where the physician had her surgery removed the medical documentation by mistake from the premises that were being cleared out and burnt it in the furnace. Violation of the Act was then noted within the control, as the physician failed to duly secure sensitive data against destruction.

■ A private physician intended to submit medical documentation to another physician (the patient changed his doctor). The physician used, as usual, a courier to deliver the documentation. Medical documentation was regularly handed over to the courier in that the physician lay the medical cards on a freely accessible table in the corridor of the polyclinic, from which the messenger always took the consignments. However, the medical cards disappeared from the table. The affected patients then justifiably complained about the procedure employed by the physician. Thus, the Act was again violated in this case, as the doctor failed to secure sensitive data of the patients against their loss.

■ Another private doctor kept a registry of medical cards of her patients in the waiting room in front of the surgery. The registry was kept in a wooden filing cabinet with separate drawers, each equipped with a lock. The patients complained that, during the opening hours, the locks on the drawers were not locked and, thus, there was a realistic possibility that unauthorized persons could peruse the medical cards or that the medical documentations could be stolen. The control revealed

that the complaint was justified and that the physician violated the Act, as she failed to duly secure sensitive data against misuse.

The results of the investigation and justified complaints of citizens about shortcomings in activities of small non-state health-care facilities prove that a number of private physicians are still unaware of the necessary requirements on protection of the patients' data and responsibility for this protection, although these aspects should be absolutely natural for them based on the principle of maintaining medical secrets. This is particularly striking in the case of information on the state of health of the patients which constitutes sensitive data, whose misuse could have deep impact on privacy of each individual. Therefore, the inspector in the area of health care will continue to concentrate on activities of private physicians.

CAMERA SURVEILLANCE SYSTEMS

In 2007, the inspectors again dealt with numerous instigations aimed against the operators of camera surveillance systems. The instigations came from various fields, particularly schools, major health-care facilities (polyclinics, hospitals), apartment buildings and workplaces of employees. A total of 23 controls were commenced, of which 14 have already been completed.

Within the controls, the inspectors repeatedly encountered camera surveillance systems whose operation did not respect the fundamental human right to protection of privacy, with the usual consequence of violation of the Personal Data Protection Act.

A vast majority of the controlled camera surveillance systems with recording equipment were established and operated for the purpose of protection of persons and property. The main and most frequent shortcoming of these camera surveillance systems lies in the fact that they are operated as a mere preventative measure, rather than as a necessary means to attain the set purpose. Of course, this would be possible, but only subject to fulfillment of some necessary statutory preconditions. Given the fact that all the controlled camera surveillance systems were operated without the consent of the monitored persons, it is necessary that they be operated either on the basis of a special law (this authorization belongs, e.g., to the Police of the Czech Republic) or on the basis of an exemption from the Personal Data Protection Act. Indeed, such an exemption allows for protecting one's justified interests; however, such protection (i.e. by acquiring a video recording) must be necessary for the operator and, simultaneously, must not infringe on the private and personal life of the monitored persons. A vast majority of operators of camera surveillance systems did not comply with the conditions of this exemption and, in that case, it was always necessary to consider the acquisition of recordings to be unlawful. Nevertheless, it must be noted that, in numerous cases, the statutory conditions were exceeded only due to unsuitable use of some cameras, or excessive scope of the acquired recordings. This scope can always be affected by the number of cameras, their position and direction, setting the time and duration of the recording, or setting the resolution capacity of the camera. However, as was shown in the controls, the operators usually use the maximum scope of acquired recordings, particularly by employing the biggest (widest) range and continual recording of data 24 hours a day by all cameras. Indeed, it is clear that, e.g., the protection of the front wall of a school does not require recordings made in the corridors of the school; that protection of parked vehicles in the parking garage of an apartment building requires recording of the cars, rather than of the stairway of the building; that, in a hospital, it is more suitable to ensure protection of the storage area for medicaments by placing a camera inside the warehouse, rather than monitoring the front door from the outside, including the entire corri-

dor. A typical example of use of cameras at a senseless time was the case of a municipal authority, where the equipment of the waiting room was "protected" by acquisition of recordings during the working hours, when the entire premises of the waiting room were watched by twelve clerks through glassed-in counters at their workplaces; however, after the working hours, the system was turned off and, thus, a potential thief would be seen neither by the officers nor by cameras.

When discussing the conclusions of the control protocols, the inspectors constantly encounter, not only lack of comprehension and knowledge of the principles of personal data protection, but also lack of respect to privacy as a whole. Arguments based on the rights guaranteed by the Charter of Fundamental Rights and Freedoms, particularly the right of every person to protection against unauthorized gathering, publication or other misuse of his personal data, is usually challenged by economic arguments of the operators (controllers).

It is also increasingly frequent that the individual elements of the camera surveillance systems are mere mock-ups or that, while some technical elements of the camera surveillance systems (cameras, wires) are installed, they are not functioning, and the entire system is thus being used as a mere "placebo". Of course, this manner of protection can be very effective, given its psychological influence on the potential offenders. However, the inspectors also encounter cases where even such a system substantially infringes on the private and personal life of persons and appears to be clearly unsuitable.

A really extreme case, with a clear impact on privacy of the monitored persons, consisted in operation of a camera surveillance system in a social care home (SCH) managed by a city ward of a statutory city. The residents of the SCH complained that the camera surveillance system preventively recorded their conduct in the entire building. The residents felt that such groundless monitoring harmed them and infringed on their fundamental right to privacy. The complaint appeared to be even more serious as social care homes contain special-purpose apartments for persons with reduced independence due to their age, chronic disease or disability.

The control revealed that a functional camera surveillance system was installed in the building and operated by the city ward of the statutory city. The cameras recorded the corridors of the buildings, including the entrances to some of the apartments. The system was in operation continuously; the signal from the cameras was transmitted to technical equipment enabling recording of the signal, at front desk of the building. The recording device (video recorder) was normally in the "recording" mode and, after termination of the recording cycle, the attendant (personnel of the SCH) replaced the recorded tapes. However, in detailed examination of the technical equipment, it was found that recording did not actually take place, as the individual components were not interconnected. Control of the tapes containing the recordings also revealed that these recordings were made without any signal, i.e. of nothing at all. This fact was also confirmed by the management of the municipal authority, which demonstrably set this non-recording regime. However, the authority intentionally failed to inform the residents of the SCH of the non-recording regime. In addition, no information was provided to the attendants of SCH, who were prohibited from changing the settings of the system and were not even aware of the fact that no recordings were in fact made.

Thus, the residents of the SCH, their visitors and persons employed in the home justifiably believed that their life in the SCH was being recorded and that their privacy was endangered, and they were concerned about how the recordings will be further treated.

It was clear in the given case that privacy of the residents of the SCH was infringed without reason. However, personal data were not processed and, therefore,

the Office was unable to effectively intervene. by imposing for instance remedial measures as the matter was outside the area of the Office's competence. The inspector recommended to the management of the municipal authority that they resolve the issue at least by communicating with the residents of the SCH. The complainants were notified of the results of the control and advised that, if the undesirable state of affairs persisted, they should deal with it before civil courts. The entire case, which is by no means unique, indicates the potential misuse of monitoring systems, with significant impacts on privacy of citizens, and could be an incentive for drawing up an appropriate legislation.

PERSONAL DATA PROCESSING IN OFFERING TRADE AND SERVICES

In 2007, the Office received an increased number of complaints aimed against marketing companies. These complaints usually draw attention to activities of marketing companies which send unsolicited mail to citizens, containing advertising materials and offers for trade and services. The citizens mostly complained that they had received such mail even though they had advised the company of their disagreement with sending offers. Within the controls of these companies, the review was also concerned, in the framework of the cooperation required by law, with the sources of their personal data, i.e. companies cooperating with the controlled firm. Activities of several companies were thus reviewed within each control.

On the basis of the controls, it was found that the issue of repeatedly sent offers had two levels.

The first, and fundamental, problem lies in the fact that a citizen (as was found in a vast majority of cases) had granted his consent to sending the offers. It was almost a rule that he had granted such consent to a company other than that from which he received the mail and about whose activity he complains. However, this need not be an unlawful procedure. In these cases, the specific consent is always examined, particularly as to whether the granted consent contains a provision on the right to transfer personal data on a citizen also to other companies. This suspicion is usually confirmed within the control, where the granted consent mostly contains a clause like "through his signature, the customer grants the consent to a transfer of the provided personal data to all business and marketing partners of our company". Then it is reviewed as to whether there is indeed a business or marketing relationship between the companies, which has always been confirmed to date. The state of affairs is thus determined and the legal assessment of the problem is very straightforward and is not favorable for the complainant. Given the fact that the data controller has the right to transfer personal data (within the scope of the name, surname and address) to a different controller for the purpose of offering trade and services, provided that the data subject (i.e. the citizen) has been informed of this procedure of the controller in advance and has not expressed disagreement with this procedure, the conduct of the controller in this case, i.e. the sender of the mail, must be considered to be authorized and not at variance with the law.

These cases should be a warning for citizens who voluntarily (and usually in consideration of some minor benefit or discount or potential inclusion in some kind of lottery) sign a generally "borderless" consent to a transfer of their personal data and are then surprised by the number of companies that send their offers to them.

The second problem is connected with cases where offers are sent in spite of disagreement of the citizen with further processing of his personal data for the purpose of offering trade and services. Pursuant to the Act, the controller may not further process personal data on a citizen (which may not exceed the scope of the

name, surname and address) if the citizen expresses his disagreement with this. This disagreement must be expressed in writing.

It has been repeatedly found that, after receiving a mail, the complainants expressed their disagreement with further offers and requested that their personal data be erased from the register of the sender. After they had received further mail, they requested that the Office provide for a remedy. Within the controls, it was verified in what form the disagreement was expressed and after what period of time after the disagreement the complainants received further consignments.

Many problems were related with compliance with the provisions of the Act on the necessity of the written form of the disagreement. The complainants were mostly unable to prove as to when and in what manner they expressed their disagreement. They either referred to a telephone call with an employee of the sender or stated that the disagreement had been sent by ordinary post or e-mail. If it was then impossible to ascertain, within the on-site investigation at the sending company, whether the company had actually received the disagreement and if the complainant was unable to find the document, it could not be stated that the activities of the sender were at variance with the Act. However, in these cases, the complainants were always informed that they should express their disagreement again in writing and keep the postal receipt. If the company continued to send the offers, they could again lodge a complaint with the Office. However, it must be stated that the inspector has not received any such repeated complaint.

There were also several instigations in cases where the complainant duly expressed disagreement with personal data processing, the posting was proved by the complainant and, nevertheless, the sender continued to send the offers. In all these cases, it was found that the complainants received further mail within three weeks of the date when they expressed their disagreement and this mail was the last obtained by these persons. In these cases, the inspector did not find violation of the Act. The reason for this legal opinion lay in the fact that, for organizational and technical reasons, it is usually impossible for marketing companies to respond immediately to every disagreement of a customer with processing of personal data so as to ensure that any mail that is already being prepared is not sent to the customer. Personal data of the customer cannot objectively be removed from processing at a time when automated technical and organizational processes are already underway, particularly printing, dispatch, distribution of mail, moreover where these activities are partly outsourced. Therefore, the inspector tolerates the mentioned period of approximately three weeks as a period during which a customer still can receive further mail, in spite of the expressed disagreement.

It should be added with respect to the issue of activities of marketing companies that the performed controls were concerned particularly with the most important and most frequently presented companies of the Czech marketing industry. Within the controls of these companies, it was not found that offers would be sent in spite of the customer's disagreement. These companies usually organize their work so as to prevent these cases. This also follows from the logic of the matter where it is clearly undesirable for a marketing company to spend money for sending offers to a dissenting customer without any purpose and, moreover, risk the potential legal problems.

ACCESS OF THE DATA SUBJECT TO INFORMATION ON USE OF PERSONAL DATA FROM THE REGISTER OF POPULATION

The right to access information on processing of personal data that is generally stipulated in Article 12 of the Personal Data Protection Act has also been reflected in practice in the provision of personal data from public administration information systems on the basis of a special law. The amended wording of Article 12, with effect from July 26, 2004, also resulted in a change in practice. This is also true for the Information System for Register of Population (hereinafter the "information system"). The information system contains data required by law on citizens and on foreigners with a permit to stay on the territory of the Czech Republic and on persons who have been granted asylum on the territory of the Czech Republic. The right of access to information is stipulated in Article 8 of Act No. 133/2000 Coll., on register of population and birth numbers and on amendments of certain acts, as amended (hereinafter the "Register of Population Act").

A request for the provision of data can be addressed to the Ministry of Interior, a regional authority or the municipal authority of a municipality with extended powers. The sample form *Application for Provision of Data from the Information System* is stipulated by a decree implementing the Register of Population Act: Decree No. 296/2004 Coll., implementing the Register of Population Act and amending Decree No. 177/2000 Coll., implementing the Register of Population Act, Act on Identity Cards and Act on Travel Documents, as amended. The information as to who and under what conditions may request such information is also published on the website of the Ministry of Interior. Extracts from the information system are provided at request; they have always the same contents and same formal layout. A request may also be made for a *record on provision of data.* The applicant obtains an overview in the form of an extract from a data file. All extracts have the same formal structure and contents. They contain a record on the date and hour of the provision and on the person to whom the data were provided. The information on the recipient of the personal data includes the name of the state body or governmental authority. The recipient may only be a body that has applied for assignment of a user authorization.

On the basis of these extracts, three persons lodged a complaint with the Office in March, April and July 2007, respectively. All the complainants believed, on the basis of an overview of information on the entity to which their personal data had been provided from the information system, that their personal data are used unlawfully. Some of them believed that, on the basis of the complaint, they would be provided with a list of persons who "misused" their personal data.

The control was concerned with the accuracy and the expressiveness of the output, i.e. provision of personal data from the information system, which was always drawn up by the Ministry of Interior. It was found that the structure, scope and substantive scope of information given in the report whereby the data subject is provided, at his request, with information on processing of personal data does not correspond, with respect to the part containing the record on the provision of data, to the contents of Article 12 (2) (d) of Act No. 101/2000 Coll., on the protection of personal data and on amendment to some acts, as amended (hereinafter the "Personal Data Protection Act"), primarily because it does not satisfy the legitimate expectation for entirety and, furthermore, because it is not comprehensible for the data subject and, finally, because they also do not comply with the requirements of Article 8 (6) of the Register of Population Act.

The extract for complainant Z. pertains to the period from July 24, 2000 to March 20, 2007, for complainant T., from July 20, 1998 to April 17, 2007, and for complainant J., it contains audit records from January 6, 1998 to April 27, 2007. Six

recipients are stated for complainant T. The Capital of Prague is mentioned as the recipient in two cases in 1999, i.e. at a time when it was not the recipient. Three recipients are specified with respect to complainant Z. and seven recipients for complainant J. The Municipal Authority of Havlíčkův Brod and the City Authority of the Capital of Prague are also specified as recipients at a time when they did not have access to the information system to which the records on the provision of data relates. Variance with the data provided to the applicant was found with respect to some audit records: e.g., of ten records where two and more entries were automatically recorded during a single day, only the first record is given; in another case, only the first record was set forth out of six records where two and more entries were automatically recorded during a single day. A difference was also found in the designation of the recipient. The Ministry of Interior itself was set forth as the recipient in all the extracts. This is the case where the personal data on the complainants were used to deal with an *application for the provision of data from the information system*. Search by the Ministry was also recorded in 14 other cases in the extracts provided to the complainants: the Ministry admitted that these records were incorrectly assigned. It also documented the use of personal data of the one of the complainants for the purpose of decision-making on an application for issuance of a lustration certificate.

Information on the provision of personal data has been provided from the information system on the basis of records kept by the Ministry within the same scope and in the same form since the time before both the Register of Population Act and the Personal Data Protection Act came into effect. This appears to be a source of problems for the data subject and, in turn, also in relation to the Personal Data Protection Act. The records on transfer of data can be unexplainable for the data subject. Their correct interpretation requires the knowledge of the development of the legislation on register of population: the information on the *provision* of data is recorded also upon each use for the needs of keeping data files with personal data, as stipulated by law, e.g. in performance of state administration in the area of identity cards or travel documents. At the time of the control, the Ministry decided that an extract from the information system would be provided from the date of effect of the Register of Population Act. On the contrary, audit records for the information system do not encompass cases of collective provision of data on the basis of the law. The volume of these sets and the scope of the personal data included in them was substantial in the previous years. At the time of the control of the Office, these sets containing personal data were processed only for the General Health Insurance Company. Other recipients of personal data from the information system are to be specifically listed in audit records in connection with their own user authorization.

On the basis of the results of the control, the Office imposed remedial measures. Each complainant was sent supplemented and corrected records on the hour and date of the provision of data pursuant to Article 8 (6) of the Register of Population Act. Compliance with the other imposed measures is directly recorded by all applicants for the provision of a *record on the provision of data*. Nevertheless, it must be borne in mind that the adopted measures are intended for the future and past shortcomings can be compensated only to certain degree. Records on the provision of data made before September 1, 2006 cannot be considered to be comprehensive. Applicants for this information from the information system should pay attention to accompanying information provided by the Ministry of Interior or become thoroughly acquainted with the legislation.

With effect from September 1, 2006, records on access are kept in the Information System for Register of Population pursuant to Article 3 (8), including: the assigned user name of the data processor; date, month and year and time of pro-

cessing; birth number of the citizen whose data is being provided; or some other information that is decisive for search for this citizen. Indeed, search for the relevant citizen is carried out through other citizens, for whom the decisive data is common and, and the reason and specific purpose of access to the information system. These records are a basis for submitting a report to the applicants. It can be assumed that the records on the provision of personal data to other recipients, giving information on communication of personal data after this date, will no longer cause similar problems.

The complaints, on the basis of which the control was performed, were also characterized by the expectation that the Office would verify the entire context of the disputed management of personal data and provide the findings. However, these expectations had no basis in the laws and, therefore, could not be satisfied. Information on processing – in the given case, an extract from the information system – directly fulfills the right of a person, as a data subject, to be informed of processing of data. The overview, which is thus obtained under the conditions stipulated by a special law, is thus a basis for potential exercise of rights vis-à-vis the controller and processor through the procedure pursuant to Article 21 of the Personal Data Protection Act. This Act grants everyone the right to respond to incomprehensible or untrue, or only inaccurate, communication from the controller and request explanation or, as appropriate, remedy of the ascertained defective situation, regardless of whether the procedure in obtaining the initial information on processing is regulated by a special law. If a request for explanation or remedy of a defective state of affairs addressed to the administrator or processor does not lead to clarification or remedy, the Office may justifiably exercise its supervisory duties.

Thus, on the one hand, the complaints about provision of information on processing of personal data in the Information System for Register of Population did not satisfy the expectations of the complainants, while, on the other hand, they contributed to the creation of preconditions for better fulfillment of the right of the data subject in processing of data, which is important for all citizens of the Czech Republic.

EMPLOYER AS DATA CONTROLLER

An employer is undoubtedly a data controller and, therefore, he may collect only personal data that are necessary for fulfillment of the specified purpose; in the given case, performance of the employer's duties. These duties include calculation of salaries, reporting to the social authority and levying social and health insurance premiums. The following personal data are necessary for this purpose: Surname; Name; All previous surnames; Date and place of birth; Birth number; Identity card number. If an employee is entitled to tax discount with respect to his children, the employer must supply, and thus process, birth numbers of children of the employees. If the employer files tax returns for his employees, he also requires information on the spouse. Calculation of salary often requires knowledge of the previous employment. The question as to whether an employee is a smoker or non-smoker should be resolved upon commencement of employment: e.g., smoking might be prohibited on the premises of the company. Other skills mentioned by the employee himself can be considered to be his advantage if better use of the employee is sought by the employer.

Therefore, we have attempted to draw up a list of personal data that are obligatory for the performance of the employees' duties: Upon commencement of employment, the employer and the future employee conclude an **employment contract**, which, pursuant to the Labour Code, is to contain identification data on the

employee (according to the Code of Administrative Procedure, the name, surname, date and place of birth and permanent address).

The employer is entitled to process the following personal data:
For registration sheets for pension insurance that are sent to the Prague Social Security Administration *(Article 37 of the Act on Organization and Implementation of Social Security):*

– date and place of birth;
– all previous surnames;
– birth number;
– permanent address.

(*If a citizen participated in pension insurance abroad and the employer is his first employer after termination of pension insurance abroad, this also includes* specification of the name and address of the foreign insurance holder and foreign insurance number.)

For accurate calculation of the salary: education, previous practice
For correct calculation of monthly advance payments on tax *(pursuant to the Act on Administration of Taxes and Fees)*: type of pension
To ascertain the exact date of the claim for retirement *(pursuant to the Act on Organization and Implementation of Social Security):* number of children (for women)
For compliance with the compulsory share of persons with disability in the total number of employees *(pursuant to Article 83 of the Act on Employment):* disability
For payment of health insurance *(pursuant to Article 10 of the Act on Public Health Insurance):* health insurance company
For reporting employment of foreigners: nationality

Declaration of a taxpayer for income tax *(pursuant to the Act on Administration of Taxes and Fees):* **If the employee claims tax relief and the spouse is employed:** Name and surname of the spouse, name and address of the employer
If the employee claims relief with respect to a child in his care: Name, surname and birth number of the child

However, the employer must approach personal data of employees as the property of the employees which has been lent to the employer only for specific, previously determined purposes stipulated by the laws (see above) and use it only for the following purposes: calculation of the salary; communication with the employee; possibility of promotion. Article 13 of the Personal Data Protection Act specifically stipulates that the controller must adopt measures preventing unauthorized or accidental access to personal data. An unauthorized person is anyone who is not legally obliged to work with the personal data. Therefore, the personnel files must be kept, e.g. in locked cabinets, available only to authorized persons. The possibility of taking part in electronic processing of the data must be restricted only to a narrow group of employees and, pursuant to the amendment to Article 13 of the Personal Data Protection Act, it is necessary to log all cases of processing of personal data (keep records thereof), where processing also includes perusal. This applies particularly in major companies that process hundreds of thousands of personal data (often very sensitive) and, nevertheless, it is not recorded who of the potential, e.g. 25 persons, actually perused them.

In smaller companies, particularly individual plants, the problem lies in the submission of salary slips to the employees, which is often carried out in a manner that allows other employees to learn the salary of the others. Information on salary and remuneration constitutes personal data that can be the subject of envy on the part of other people and, therefore, it may not be disclosed to other employees.

PERSONAL DATA FOR SOCIOLOGICAL RESEARCH

Sociologists often obtain data for their sociological research through questionnaires which they consider to be anonymous as they do not request basic identification data. However, the anonymousness of these data must be carefully considered. According to the definition stipulated by the Personal Data Protection Act, personal data means any information relating to identified or identifiable data subject. A person could perhaps become identifiable simply on the basis of a greater scope of personal data that do not, in themselves, identify the given person – e.g. an incorrectly specified answer. This problem is especially apparent in relation to children which, on the one hand, are not yet able to appreciate the risk and, therefore, cannot themselves provide consent to processing of their personal data, while, on the other hand, they can incorrectly understand a question and, in fact, identify themselves through the answer (e.g. father's job: President of the Republic). In the current world of investigative journalism, it is necessary to consider the risk of whether it would not be worthwhile for a journalist, if overly sensitive questions are posed (drugs, sexual life), to look up a specific child from the set of personal data obtained through the questionnaire.

TRAVEL AGENCY

A decision on imposing a fine of CZK 400 thousand on a private travel agency caused a number of subsequent actions with the amount of the fine as common denominator. In addition to the fact that, undoubtedly, the defective state of affairs was remedied and protection of personal data of hundreds of thousands of citizens was improved on the basis of the control and administrative proceedings, it was particularly ensured that, not only the owners and managers, but also all employees of this company finally acknowledged the nature of the aspect of personal data protection.

It must be noted that a very high number of personal data are processed in tourism. Personal data are processed, not only on the citizens of the Czech Republic, but also on nationals of third countries; in tourism, some personal data must be transferred not only amongst the individual service providers but abroad as well. Almost every citizen traveled at least once with one of travel agencies during the last fifteen years. Unfortunately, the feeling still prevails that travel agencies have only a minimum of information on their passengers, which cannot actually be misused. Indeed, the travel agreement includes "only the name, surname, home address and telephone number". However, further information, without which travel services cannot be provided, is then assigned to these identification details – information on with whom, where and for what price the client will be traveling. However, this may also include information on the employer who contributes to the price of the travel, information on the requirements on accommodation, catering and travel that can be based, for example, on the state of health or religious customs related to meals. Moreover, this also includes information that the travel agencies collect in relation to procurement of visas, insurance, air tickets, etc. and which they merely submit to insurance companies, consulates and other entities. All these

data are then often accumulated in the travel agency and, for some clients using fidelity programs, the individual data are often repeatedly provided and renewed. In the case of the controlled travel agency, which records personal data of all its clients in its database, i.e. for the last fifteen years, it would be possible to ascertain, with respect to some clients, e.g. changes in the place of residence, telephone number and employer, birth of children, as well as divorce or marriage, etc. The control itself revealed that the travel agency substantially underestimated management of personal data upon their transfer abroad, particularly to "high-risk" countries.

Thus, the risk of misuse cannot be ruled out. In spite of the most sophisticated securing of electronic databases, including restriction of access to the stored information, this danger grows proportionally to the quantity of processed data and with the growth of the travel agency. Remote electronic access to the client database, forwarding personal data in the provision of ordered services amongst the individual branches, contractual vendors and individual service suppliers, moreover without any encryption of the messages sent via normal e-mail correspondence, with the possible personal misconduct or confusion of addresses, can result in a loss of control over the managed personal data. In the case of the controlled travel agency, it can also be assumed that information on traveling politicians or "celebrities" could be, in some cases, misused, e.g. by the tabloids. Sole information that somebody will be traveling with the entire family abroad at a certain time could be a hint for thieves. This is true even without respect to the potential additional piece of information that a certain person bought an expensive holiday trip and, thus, more valuables can be expected in his apartment. This can be prevented, in addition to the relevant laws, by not maintaining information on clients within such a large scope. This is the primary task of each data controller: to answer himself the question as to whether and for what purpose he will store the individual personal data - whether they would be used, e.g. to address clients with a specific business offer or whether they would be used for control of compliance with the criteria in the provision of fidelity discounts on various specific offers, etc. In summary, travel agencies belong amongst the biggest personal data processors in the Czech Republic, because travel services cannot be provided without personal data at all.

A problem in itself is related to the fulfillment of the information duty and the absolutely neglected right of a citizen to have his personal data handled only with his knowledge and consent. Based on the control at the travel agency, as well as other controls, it can be concluded that, not only private companies, but also governmental and municipal authorities are still not sufficiently aware that the data subject, i.e. an individual, has the right to make independent decisions on his personal data and that he has the natural right to know by whom, when and how his personal data are handled, and why and for what purpose they are in their database. Moreover, this right may be limited only by law. Controllers often believe that, if they have already obtained some personal data, it is solely upon their discretion as to how they will manage these data. They are actually unaware of the fact that, by unauthorized processing of personal data, they infringe on privacy of a specific person. On the other side of the coin, there is the fact that those who manage personal data in the position of the controller do not realize that, on the contrary, in numerous other situations, they find themselves in the position of data subjects.

Another important aspect of the results of the decision-making activities of the Office lies in the fact that the decision on imposing a fine on a travel agency initiated a number of meetings, questions and requests for consultations and for information from other entities in tourism. The Office was addressed by both associations which associate a vast majority of travel agencies in the Czech Republic. The Office provided direct consultations to the biggest travel agencies. The em-

ployees of the Office were sent to lectures and workshops to explain to representatives of travel agencies the basic duties imposed by the Act in personal data processing. Given the attitude of the representatives of the two associations of travel agencies, it was thus possible to address a majority of businesses in the area of tourism. Unfortunately, it must be stated that negotiations with the representatives of the individual travel agencies revealed minimum awareness of the duties imposed by the Act on them, as the controllers of personal data, in their processing. Consequently, it can be assumed that only a fine of a higher order has forced the individual entities in a sector as important as tourism to consistently deal with the aspects of personal data protection. Based on this experience, the Office can conclude that, in order to raise awareness in the area of personal data protection, it would suffice to substantially increase the amount of the imposed fines. While this could be one of the options, it must not be neglected that negotiations with the representatives of professional and similar associations are a way of introducing protection of personal data in the practice of individual companies and institutions. The fact that this manner of exerting influence is correct was also shown in negotiations with the representatives of schools in dealing with the issue of use of camera surveillance systems in schools.

A fine in the amount of CZK 400 thousand does not belong among the highest imposed by the Office to date. While this is not a negligible amount, it attained 20 % of the upper limit of the statutory range and, therefore, it can be considered to be close to the bottom limit. Nevertheless, the amount of the fine incited a response, not only from the travel agency itself, but also from other travel agencies. It is logical that the amount could seem high and inappropriate to representatives of tourism who do not have available more detailed information. Nevertheless, in the decision-making of the Office, this was only a logical climax to supervisory activities. The imposing of a relatively high amount is a result of the fact that the travel agency failed to adopt all the remedial measures imposed thereon in the previous control. It paid the previous fine of CZK 20 thousand without any problems, but it failed to remedy the unlawful state of affairs. The Office took this fact into consideration in making the decision on the amount of the fine. The objective was to bring an entity continuously breaching the law to order. Without thorough control and without the possibility of enforcing the fulfillment of the imposed remedial measures, the control activities would be futile.

It can be concluded on the basis of a single control and the subsequent administrative proceedings that thorough supervision in the form of control, consistent enforcement of the remedial measures aimed at eliminating mistakes in processing of personal data, as well as suitable choice of means to ensure remedy, including higher amounts of fines, is a way of ensuring remedy of an illegal state of affairs and extension of legal literacy in the area of personal data.

CZECH OFFICE FOR SURVEYING, MAPPING AND CADASTRE

A control carried out in 2007 was concerned with assessment of conformity of the current legislation on the Land Registry of the Czech Republic (hereinafter the “Land Registry”) with the principles of personal data protection.

The strategy of full digitization of the Land Registry was adopted In the first half of the 1990s on the basis of a resolution of the Government. Its objective was, not only to supplement the data base of the Land Registry, but also to create a modern and improved information system of the Land Registry that would correspond to the current and prospective needs of the state and would be comparable with similar systems in the countries of the European Union.

The benefits of the improved information system of the Land Registry were to include, in particular:

a) acceleration and improvement of activities of cadastral authorities in keeping the Land Registry;
b) accessibility of information from the Land Registry by remote access to the data via the internet;
c) possibility to obtain data independently of the place of inquiry and of the place of storage; it will be possible to obtain data from any cadastral area of the Czech Republic at any cadastral authority; in justified cases, it will be possible to obtain data on ownership of real estate by natural and legal persons from the territory of the entire Czech Republic (for the needs of the courts, Ministry of Interior, Ministry of Finance).

However, in the opinion of the relevant inspector, upon ordering the implementation of the approved strategy, account should have been taken of the fact that Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which provides for a general legal framework of the EU for application of the principles of personal data protection, must be transposed to the Czech legislation in relation to accession of the Czech Republic to the EU. In the opinion of the inspector performing the control, this is not an extraordinary procedure, which is documented by some publicly available information in some other EU Member States (e.g., in Germany, personal data protection is the main reason why the Land Registry may be perused only if legal interest exists; justification by the existence of business relations is inadequate. In France and Spain, written information from the Land Registry is provided with the consent of the owner.).

Persons requesting a copy from the collection of documents, which contains a decision of governmental authorities, contracts and other deeds, on the basis of which the relevant entry was made in the Land Registry, are not required to submit an application; they merely pay the relevant administrative fee for authentication of the copy. Through this procedure both personal data of persons who have the ownership title or some other relation to the real estate and personal data of persons who necessarily does not have any relationship to the relevant real estate are disclosed. However, pursuant to Article 10 of the Personal Data Protection Act, the controller and processor must ensure that the rights of the data subject, in particular, the right to preservation of human dignity, are not infringed upon and must also ensure that the private and personal life of the data subject is protected against unauthorized interference.

Pursuant to Article 5 (1) (d) of the Personal Data Protection Act, the controller must collect personal data corresponding exclusively to the specified purpose and in an extent that is necessary for fulfillment of the specified purpose. As follows from Article 1 of the Cadastral Act, the Land Registry is kept as a set of data on real estate, including records of ownership titles and other rights to real estate. However, the purposes of keeping the registry are specified very extensively and generally, which contributes to their misuse for obtaining information of a purely private nature, misuse of which is strictly safeguarded by other legislation. As example of a purpose specified in such a manner may serve notably the “creation of other information systems”, which is absolutely inadmissible as a purpose of its own from the viewpoint of the principles of protection of personal data kept in the registry and is at variance with the EU regulations concerning protection of privacy. In this respect, reference can be made particularly to Article 6 of Directive 95/46/EC, which stipulates (similar to Article 5 of the Personal Data Protection Act) that personal data must be processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in a way incom-

patible with those purposes; personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

As regards the fulfillment of the notification duty borne by natural persons in case of a change in shared data, in the opinion of the inspector, the existence of Article 5 of Decree No. 111/2001 Coll. creates sufficient legal conditions for performance of the controller's legal duty stipulated by the Personal Data Protection Act in that *"If there is a change in data shared in the registry with respect to a natural person recorded in the register of population and, simultaneously, as the owner or some other authorized person, in the registry, it shall suffice if this person notifies the change to the filing department for the register of population. His/her notification duty with respect to the change in these data shall thus be considered to be fulfilled in relation to the administrator of the registry."*

In the opinion of the inspector, this legal regulation should contribute, not only to reduction of the administrative burden borne by the controlled entity in relation to changes in personal data of persons registered in the Land Registry, but also to substantial reduction of the quantity of personal data recorded in the collection of documents.

The inspector thus came to the conclusion that, while the Land Registry is kept in accordance with the special Act on the Land Registry, it is at variance with the general law stipulating the conditions for processing of personal data.

Furthermore, it must be stated in this respect that disclosure of personal data to individual natural persons exclusively for their needs, within any scope, is not at variance with the Personal Data Protection Act, because it is stipulated, in accordance with Directive 95/46/EC and in accordance with Article 3 (3) of the Personal Data Protection Act, that the Act does not apply to personal data processing carried out by natural persons exclusively for personal needs. However, the Act must apply in all other cases.

SPAM AND UNSOLICITED COMMERCIAL COMMUNICATIONS

The attention and time dedicated to spam in the media, as well as in daily life, has been constantly increasing. Various statistics are regularly published stating the percentage of spam on the usual electronic mail. The information differs particularly according to what the author considers to be spam and how much he intends to "shock" the public. Is this 80 % or 90 % or some other figure? A special OECD task force, in which the Office participated, created a well-arranged brochure (toolkit) describing this issue, including the possible remedies. Indeed, spam measurement was one of the discussed topics, as it is necessary to find out whether and how effective the adopted measures will be. The first problem arose already with respect to the actual subject of measurement. It is clear that if all unsolicited mail is considered to be spam, the percentage will be very high, as most e-mails are unsolicited. A majority of personal mail is, in fact, unsolicited and only few persons have available demonstrable consent of the recipient before they send him a message. However, nobody conceives spam this way. If the criterion is to lie in the degree of nuisance, this is again a very individual question.

For example, we have received a complaint about "spam" sent from the server "Classmates". Thus, there are people who are bothered by the fact that their former classmates invite them to a pub and, on the other hand, there are those who welcome an offer of cheap toners, even though they have not asked for it. Thus, this is always a matter of opinion, which can hardly be resolved by spam filters in all possible situations. Moreover, spam filters themselves breach protection of privacy, as they require that the administrators read these messages, which are often personal.

From the viewpoint of the Office, its control function in the area of spam is clear. The penalties which we impose are related to business offers or advertising communications sent by Czech legal entities to persons who are not customers of the offering party or have not provided their prior consent to be addressed with offers. These two categories of messages must be clearly distinguished. The unsolicited commercial communications have a rather different nature in the Czech environment and general "spam" criteria cannot be applied. In the case of a commercial offer sent by a Czech company with the possibility of opting out, the latter option must first be used, and if this leads to no effect and the offers continue to come, the relevant company must be appropriately "advised". However, prior to lodging a complaint, it is necessary to recall whether we have bought something after all, or whether we have not obtained something "free of charge" or whether we have not been lured by an offer somewhere. A number of cases end with the controlled entity submitting the Office documents on registration, on use of a product or on the fact that the relevant person has been their long-term customer. There are cases where the Office achieves removal of the given person from the database, only for this person to register again. There are people who have forgotten their original password and, thus, register again under a new password. There are cases where the Office found a complainant six times in a single database, always under a different user name, but with the same electronic address. Of course, some blame must be placed on the registration software of the particular company; nevertheless, the Office encourages companies not to pay attention to the e–mail address, as people sometimes have different receiving and sending addresses and, therefore, an e-mail should be assigned a customer code or some other unique identification code.

While in the neighboring European countries, legislation is derived from the same Directive, it is important from the viewpoint of complaints whether any damage or harm has been incurred and whether bulk mails are concerned. The authorities do not intervene unless the number of complaints reaches a certain level (e.g., 40 in the Netherlands, etc.). The fact that the inspectors of the Office have no possibility to obtain direct information on the sender from the relevant internet providers, together with their duty to deal with every single complaint, puts them into a difficult position. Nevertheless, thanks to an increase in the number of employees of the inspectorate entrusted with the agenda of unsolicited commercial communications and personal data, it was possible to reduce the period between the submission of a complaint and its resolving from approx. 16 to 3 months. In substance, it is impossible to handle the complaints within a shorter deadline and this would not be reasonable as it is first necessary to wait whether more complaints would be lodged against the same sender; the actual control process then takes almost two months.

The complaints are submitted through an anonymous internet form, which is easy to counterfeit and whose potential modification would place high technical requirements on the complainant. The forms for submission of complaints used in the neighboring countries could serve as an example. These forms consist of several pages and are very detailed; in addition to a number of technical details, they also include verified identity of the complainant. For many complainants, the case is closed by filling in our form and they do not realize the need for keeping the subject of the complaint, i.e. the relevant unsolicited commercial communication in an unchanged form until the case is finally closed which could take even several years if it is brought before the courts.

II. Findings obtained by inspectors in administrative proceedings

In 2007, the inspectors of the Office also continued the practice from 2006, when they were allowed to pursue administrative proceedings, in which they are able to reflect on the findings obtained in their controls. The institute of summary proceeding was employed in a number of cases. This practice has shown to be suitable, particularly because it enables to shorten the process of the administrative proceedings. Administrative proceedings pursued by the inspectors have proven to be effective, as it made possible to decide on the gravity of the offense, and thus also on the amount of the fine with thorough knowledge of the case.

The administrative proceedings were initiated by the inspectors on the basis of their control findings; either on the basis of controls performed according to the control plan or based on instigations from third parties.

In 2007, the inspectors of the Office pursued a total of 108 administrative proceedings, of which 96 took the form of an order pursuant to Article 150 of the Code of Administrative Procedure. 102 administrative proceedings were completed through a final decision in 2007. Fines in total amount of CZK 4,668,500 were imposed in administrative proceedings; of this amount, the obliged entities paid CZK 1,563,500 in 2007. The highest amount imposed in 2007 equaled CZK 1,750,000; the highest fine imposed and paid in 2007 amounted to CZK 400,000.

Administrative proceedings (71 of the total number of 108) were pursued in cases of breach of duties stipulated by Act No. 480/2004 Coll., on certain services of the information society and on amendment to some acts (the Certain Services of Information Society Act), as amended, in the area of unsolicited commercial communications. Fines in a substantial amount were imposed in 5 cases for repeated violation of the Act.

In cases where breach of the duties stipulated by the Personal Data Protection Act was found, the administrative proceedings were pursued particularly in case of breach of the duties stipulated in:

- Article 5 (1) (c), where the controller failed to update personal data or processed inaccurate personal data;
- Article 5 (1) (d), where the controller or processor collected personal data on a data subject to an extent greater than necessary for fulfillment of the specified purpose. This finding was made both in the private and public sectors;
- Article 5 (2), where the controller processed personal data without consent of the data subject;
- Article 11 (1), where the controller failed to inform the data subjects of the scope in which and the purpose for which the personal data would be processed, who and in what manner would process the personal data and to whom the personal data could be disclosed; the controller failed to inform them of their right of access to personal data and the right to have their personal data rectified, as well as on other rights stipulated in Article 21;
- Article 11 (2), where the controller failed to instruct the data subject on whether the provision of the personal data is obligatory or voluntary;
- Article 13 (1), where the controller or processor failed to fulfill the duty to adopt measures preventing unauthorized or accidental access to personal data, their change, destruction or loss, unauthorized transmission and other unauthorized processing, as well as other misuse of personal data.

In 8 cases, a procedural fine was imposed, in the form of an order, in administrative proceedings for failure to provide cooperation necessary to perform control within the meaning of Article 30 of the Personal Data Protection Act.

ADMINISTRATIVE PROCEEDINGS PURSUED BY INSPECTORS

Both summary proceedings in the form of an order and ordinary administrative proceedings were employed during 2007. The decision on the form of the administrative proceedings was made particularly according to the gravity of the violation, but also on the basis of experience obtained during the control in relation to the controlled person. If the controlled person showed interest in remedying the unlawful state of affairs already during the control and one-time and negligent violation of the Act was involved, the option of pursuing administrative proceedings in the form of an order showed to be more effective.

The experience obtained during the performance of control is also reflected in considerations on obligatory imposing of fines. The imposing of a financial penalty does not always reflect fairness, but is rather solely application of a statutory provision on administrative punishment. This was clear in two administrative proceedings which followed up on the previous control. In both cases, only a one-time and marginal violation was proved and this was caused by a lack of comprehension on the part of specific employees. In the first case, a photograph of an employee was displayed on the premises of the company.

While it is true that the employee did not give consent to such processing, he was familiar to all the employees of the company and, thus, he incurred no harm whatsoever.

In the second case, the employees of non-medical professions in health care were sent an offer to subscribe to a professional journal concerned solely with the aspects of health care. However, the relevant persons were not informed in advance that the personal data would also be used for this activity. Although this constitutes breach of the duties imposed by the law, it is a fact that, in practice, this journal is subscribed to only by persons who perform non-medical professions in health care.

Subsequent administrative proceedings were held in both these cases and fines were imposed. However, it was clear that one of the basic principles in imposing fines, i.e. the educational principle, was not fulfilled by the imposing of the fine, but rather already by the previous discussion of the violation of the Act within the control.

The aforementioned experience can be summarized in a simple statement. The pursuing of administrative proceedings by an inspector, i.e. an official, who has performed the control activities in the same case, proved to be efficient, particularly because evidence is collected already during the control process also with respect to the subsequent administrative proceedings and because thorough knowledge of the case can be used in assessing the gravity of the conduct and, thus, the amount of the fine.

Of the number of administrative proceedings pursued within the inspectorate, attention was paid to proceedings against a company operating a camera surveillance system at the workplace of its client center. Already during the control, and subsequently in the administrative proceedings, it was proven that the cameras were used to document the activities of own employees of the company who were present at the workplace during the working hours, without having obtained their consent and without this being necessary for the activities of the company; the surveillance was used to monitor their working performance. This company used the camera surveillance system only during the working hours. It did not at all serve

for the declared purpose of preventing theft, protection of property or protection of health of the employees. The records were evaluated only from the viewpoint of working performance, i.e. monitoring of daily activities of the employees. Subsequently, they were used for their mobbing. This "peeping" had nothing in common with protection of the rights and legally protected interests of the employer who thus grossly infringed on personal rights of the employees, not only without their consent, but even in spite of their protests. Through this conduct, the employer not only breached the duties stipulated by the Personal Data Protection Act, but he also violated the Labor Code, which allows the employer to monitor the employees only in very exceptional cases. The management of the company did not at all consider the protests of the employees, who requested that the cameras be removed, or the fact that it infringed on fundamental constitutional rights of its employees. A decision on a fine in the amount of CZK 200 thousand was made in this case. This decision was fully upheld in the subsequent remonstrance proceeding.

Good knowledge of the conclusions of the performed control was also used in subsequent administrative proceedings against three important associated financial companies. These companies decided, within their business group, that they would identify all persons calling these companies. This decision led to a situation where a call could not take place without identification of the caller. In the administrative proceedings, it was proven that the decision of the management of all three companies did not take into account that not all callers were interested in identifying themselves and being registered in a database and that not all callers were or wanted to be potential customers. Together with forced identification of the callers, all telephone calls were recorded. Each of the companies thus breached, by its conduct, the duties stipulated by the Personal Data Protection Act as it processed personal data for purposes that were not necessary; they processed personal data of the callers without allowing them to express their consent or dissent and without providing them with the required information on the purpose and extent of processed personal data. Personal data on persons who had no legal relationship to any of these companies were thus collected. Again, the decision on identifying and monitoring of the callers was affected by the fact that obtaining of information for business activities was preferred to the right of an individual to protection of his privacy.

In 2007, based on the previous control findings, administrative proceedings were pursued against a non-state health-care facility where it was proven that the facility, as a data controller, failed to adequately secure the medical documentation of approx. 2 thousand patients. At variance, not only with the Personal Data Protection Act, but also with the Act on Health of the Population, which defines the duties of health-care facilities in management of medical documentation, this medical documentation was discarded at a waste collection site. The fine imposed for the demonstrated administrative tort, equal to CZK 1,750,000, was the second highest fine imposed by the Office since its establishment. When determining the amount of the penalty, account was taken, not only of the gravity of the breach of the duties on the part of the health-care facility, but also to the overall lax approach of the management of this facility to protection of data and information maintained in the medical documentation.

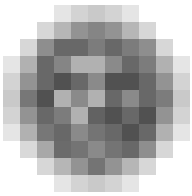
The institute of an order that is issued in summary proceedings following up on a completed control proved to be very effective during the previous year in the area of unsolicited commercial communications. This trend continued in 2007.

In 2007, inspectorate IV pursued a total of 71 administrative proceedings, of which 70 took the form of an order pursuant to Article 150 of the Code of Administrative Procedure. A protest was lodged only against 2 orders; appeal was sub-

mitted in 1 case. In 7 cases, a procedural fine was imposed, through an order, for failure to provide cooperation necessary for the control; in one of these cases, the necessary documents were subsequently supplied and the control could thus be completed. The Office encounters cases where certain entities breach of the provisions of Act No. 480/2004 Coll.; i.e., they send unsolicited commercial communications repeatedly, in spite of the fact that a fine has been imposed on them. It must be noted that, in case of repeated breach, the amounts of the fines are substantially higher. In 5 cases, the Office took this fact into consideration in decision-making on the amount of the fine.

Thus, 69 proceedings were closed through a final decision in 2007; fines were imposed in the total amount of CZK 437,000.

One of the entities continues to send commercial communications without having the consent of the addressees or them being its customers, in spite of the fact that two fines have already been imposed on this entity (the total amount of the two fines equaled CZK 81,000). Act No. 480/2004 Coll. does not provide for any other possibility of ensuring a remedy than imposing a fine.



Performance of Control, Supervisory and Administrative Competence of the Office

I. General

Activities of the Section of Supervisory Activities of the Office concentrate on the following:

Acceptance of instigations, complaints and notifications related to violation of the Personal Data Protection Act and handling thereof, particularly in the first phase of their assessment – these activities are carried out by the Complaints and Consultations Department;

Acceptance of notifications related to personal data processing pursuant to Article 16 of the Personal Data Protection Act and pursuing of registration proceedings and acceptance of instigations pursuant to Article 27 of the Act with respect to the intention to transfer personal data to other countries and their assessment, including decision-making on permitting or not permitting this intention – these activities are carried out by the Registration Division;

Acceptance and handling of applications for the provision of information pursuant to Act No. 106/1999 Coll., on free access to information, as amended (hereinafter the "Act on Free Access to Information") – these activities are carried out by the office of the Deputy President;

Administrative support for control activities of the Office performed by inspectors – these activities are carried out by inspectorates;

Acceptance of complaints about the procedure of officers of the Office lodged pursuant to Article 175 of Act No. 500/2006 Coll., the Code of Administrative Procedure, amended (hereinafter the "Code of Administrative Procedure") – these activities are carried out by the office of the Deputy President;

Performance of administrative activities related to the imposing of fines in administrative and misdemeanor proceedings pursuant to the Code of Administrative Procedure and the Personal Data Protection Act, or special legal regulations, as appropriate. These activities are carried out at the Office, in the first instance, by several officially authorized persons; these activities are performed by the inspectors of the Office particularly in those cases where penalty proceedings are to follow up on the results of the control proceedings. In addition to inspectors, these activities are also carried out by the Administrative Proceedings Department;

Performance of legislative activities taking place both within the framework of the external intersectoral commentary procedure and within the creation of own legislative proposals of the Office, also including internal regulations – these activities are ensured by the Legislative and EU Law Division;

Performance of analytical and strategic activities in support of other activities and preparation of second-instance decisions issued by the President of the Office and creation of opinions and statements, particularly in cases where the decisions of the President of the Office are challenged before the courts – these activities are ensured by the Legal Support Department.

Supervision over compliance with the principles of personal data protection in the Schengen Information System, to which the Czech Republic acceded on December 21, 2007, is being performed by the newly established Schengen Cooperation and the 3rd Pillar Department. This Department also provides for and coordinates the cooperation with other bodies that participate in the operation of the Schengen Information System.

In addition to the general public itself, the activities of the Section of Supervisory Activities are initiated particularly by the President of the Office; with respect to control activities, the President addresses directly the individual inspectors of the Office and requests that they commence control in cases of breach of privacy in personal data processing that are important for society and where it is necessary to achieve, in a rapid and effective manner, the cessation of the illegal conduct of the controller or processor and quickly remedy the illegal state of affairs. The following controls were initiated in this manner in 2007:

- On May 22, 2007, the President of the Office decided on investigation of suspected illegal personal data processing in relation to the well-known case of a tortured boy. The investigation resulted in putting the case aside.

- On June 19, 2007, the President of the Office resolved to verify the manner of processing of genetic data by Genomac International, s.r.o. The control had not been completed by the end of 2007.

- On July 13, 2007, the President of the Office resolved to investigate the suspected illegal personal data processing by The Fund for Children in Need. The control is underway and its scope will be extended on the basis of further complaints.

- On October 17, 2007, the President of the Office resolved to verify the suspicion of illegal personal data processing by the Ministry of Interior of the Czech Republic in relation to implementation of a project aimed at the area of prevention of youth crime. The control is pending and the control findings are currently being processed.

Uncompleted controls initiated by the President of the Office in 2006:

- *Criminological Institute in Prague; processing of a DNA database.*
  The control of the National DNA Database was concerned with the conditions for keeping this register within the limits of the Act on the Police of the Czech Republic and the Personal Data Protection Act. The control findings are currently being processed.

- *České aerolinie, a.s.; personal data processing in relation to transfer of personal data of passengers to the U.S.A.*
- *České dráhy, a.s.; processing of personal data of the In-karta service's subscibers.*

The control, which was based, inter alia, on instigations from the subscribers received by the Office, was concerned with processing of personal data of passengers in relation to implementation of the Czech Railways project entitled "In-karta". This is a technically complex process of processing of personal data of natural persons – the subscribers to the services related to possession of an identification card using the RFID chip technology, within a large scope. The control revealed that it would be necessary to modify the plans of the Czech Railways, as the data controller, with regard to the conditions of personal data protection and other problems related to this project.

- *Radio Free Europe/Radio Liberty; processing of personal data in relation to operation of a camera surveillance system.*
  The control is pending. Given the fact that information that has fundamental influence on the security, not only of the Radio Free Europe/Radio Liberty premises, but also of the center of the Capital of Prague, is being treated within the control, the control is being performed under a special regime, with respect to both the inspectors and the controlled entity.

  Individual ministries are often addressed on the instigation of the President of the Office; given the current state of the legislation and certain steps in application of legal regulations that do not always absolutely unambiguously respect the principles of personal data protection, it is necessary to negotiate with these ministries on a possible change in the current state of affairs. These activities were related particularly to the following aspects in 2007:

- Potential cooperation between the Office and the Ministry of Labour and Social Affairs and with the State Labour Inspection Office in the area of control of operation of camera surveillance systems at workplaces.
- Cooperation with the Ministry of Education, Youth and Sports and the Czech School Inspectorate in the area of operation of monitoring systems at schools.
- Cooperation with the Ministry of Health in the area of protection of patients' privacy in processing of their personal data.
- Cooperation with the Chamber of Distrainers of the Czech Republic in the area of procedures of judicial distrainers, where movable things (mobile telephones, personal computers) containing personal data are seized.
- Cooperation with the Ministry of Interior in implementation of the plan for making public administration accessible as a service for citizens through the CzechPoint project, which is a part of the new strategy in the area of E-government and its services.
- Cooperation with the Ministry of Justice in the procedure related to the planned electronic operation of the Commercial Register and its services, with regard to privacy protection of natural persons whose personal data are publicly accessible information, and active participation of the Office in implementation of the E-justice project.

These activities of the President of the Office are also supported by the fact that, in 2007, he became a member of three expert bodies of the State: **the Government Council for Human Rights, the Government Council for the Information Society and the Standing Commission on Privacy Protection in the Senate**. In 2007, an external meeting of the Standing Commission on Privacy Protection took place directly in the building of the Office and the members of the Commission thus had the opportunity to meet the inspectors of the Office and the senior officers who presented their experience with application of the Personal Data Protection Act in practice.

II. Control activities

Active cooperation of the Section of Supervisory Activities with the inspectors of the Office in the area of control activities has been useful particularly in the creation of the *Plans of Control Activities of the Office*. Its general part specified the following main topics for control activities of the inspectors of the Office in 2007:

- Public administration information systems
- Personal data processing with the use of camera surveillance systems
- Preparedness of the Czech Republic for accession to the Schengen Information System:
- Transport systems in the Czech Republic and personal data processing in their operation
- Area of justice, state attorneys and other entities engaged or participating in the process of personal data processing in this sector

A special part of the plan of control activities then determined the following **specific planned controls** to be performed by the inspectors of the Office in 2007:

Processing of personal data of holders and drivers of vehicles in operation of the electronic toll system:

The control concentrated on compliance with the conditions for drivers' personal data processing in relation to the collection of the toll for use of motorways and on the question whether the processed personal data are appropriate as regards their scope and purpose of processing and whether they are not disclosed to other entities. The control was closed without finding any breach of the data controller's duty in personal data processing.

Personal data processing in relation to the visa proceedings at embassies of the Czech Republic:

The following controls took place based on a recommendation provided by the expert commission for Schengen evaluation of new Member States in the area of personal data protection:

A control at the Embassy of the Czech Republic in Kiev, concerned with the visa proceedings at embassies. In relation to this control, the competent inspector suggested to the Ministry of Foreign Affairs, as the entity responsible for compliance with the conditions for personal data processing, to modify the current procedure in the provision of information to visa applicants with respect to the second sentence of Article 11 (1) of the Personal Data Protection Act.

Control at the General Consulate in Saint Petersburg, aimed at verification of the processed data security and checking the flows of data included with visa applications from consulates, and at ascertaining whether they comply with the statutory regulations and, simultaneously, the requirements of the Schengen catalogue and whether they are in conformity with the "Best Practices" in visa granting.

The verification of the visa granting procedures also included a control at the Immigration Police.

Personal data processing in operation of the Road Vehicles Register

The control was carried out in the Statutory City of O., which performs the activities of a governmental authority in the processing and use of personal data from the road vehicles register. No violation of the Personal Data Protection Act by the controlled entity was found in relation to maintenance of the electronic and documentary parts of the register.

Personal data processing in relation to In-karta chip cards:

As mentioned above, the control was concerned with processing of personal data of passengers in relation to implementation of a Czech Railways project. Given the contemplated interconnection of user services intended for the passengers in suburban mass transportation, the control will also take place in 2008.

Personal data processing by prosecuting bodies

The control took place at a District State Attorney's Office and was concerned with compliance with the duties in personal data processing in criminal proceedings and their potential further use in other information systems with respect to Article 13 of the Personal Data Protection Act. The control did not reveal any breach of duties in personal data processing pursuant to the Act.

Personal data processing with the use of camera surveillance systems at schools

A control of a camera surveillance system at a Prague elementary school is underway.

Processing of personal data of visitors to the Chamber of Deputies:

A control at the Office of the Chamber of Deputies was concerned with the records of the visitors of the buildings of the Chamber of Deputies, the type of personal data processed of the visitors and the data retention period. The control was completed, but the controlled entity lodged objections against the control protocol.

Personal data processing and compliance with the conditions for their protection in relation to administration of the Land Registry:

The control was concerned with specification of the limits for the conditions of personal data processing in relation to the Cadastral Act, which considers the Land Registry to be a publicly accessible register, and for the conditions of personal data processing pursuant to the general Personal Data Protection Act, which requires that any interferences with privacy of natural persons be transparent and that they clearly follow from a public interest promoted in society.

Personal data processing with the use of camera surveillance systems by the municipal police:

Register of records of memory cards in vehicles equipped with recording equipment was checked within the control performed in the statutory city of O. No violation of the Personal Data Protection Act was found in the processing that has been functioning as a part of the road vehicles register since July 1, 2007.

Personal data processing by prosecuting bodies:

A control performed at a district court was concerned particularly with the exercise of the rights and obligations stipulated in Articles 5, 9, 11 and 13 of the Act. The facts ascertained during the control revealed that the district court (data controller) proceeded at variance with the Act in personal data processing, as it processed sensitive data without the data subject having granted its express consent to the processing and having been informed upon granting the consent as to what was the purpose of the processing and for what personal data the consent was being granted, to which controller and for what period of time. The control revealed that the mentioned conduct of the district court led to breach of Article 9 (a) of the Act.

Personal data processing with the use of camera surveillance systems in health care:

Control aimed at monitoring systems is taking place in a health-care facility.

Processing of personal data of clients of the State Fund for Housing Development:

The control was postponed to 2008.

Personal data processing in relation to operation of a camera surveillance system in an art gallery:

The ,purpose of the control is to verify the manner of processing of personal data of persons who are present on the monitored premises.

The Section of Supervisory Activities, in cooperation with the inspectors of the Office, provides administrative support for the *Objections Board of Inspectors*, which is a newly established advisory body of the President of the Office authorized to deal with objections of the controlled entities against the results of controls, as contained in the control protocols, and claims of prejudice raised against an inspector of the Office.

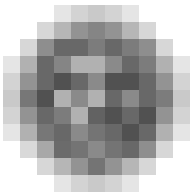
The board, as a special body, met a total of eleven times in 2007. Overall, it discussed the objections of thirteen controlled entities in 2007 and proposed the manner of resolving these objections to the President of the Office.

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

In 2007, the Office received a total of four requests for information within the meaning of the Act on Free Access to Information. The Office did not satisfied three of these requests in accordance with Article 15 of the Act on Free Access to Information. The Office satisfied one request and, subsequently, in accordance with Article 5 (3) of the Act on Free Access to Information published the contents of the provided information on its website in an anonymous form.

IV. Complaints handling pursuant to Article 175 of the Code of Administrative Procedure

In 2007, the Office received a total of twenty-seven instigations which it evaluated and subsequently handled as a complaint pursuant to Article 175 of Act No. 500/2004 Coll., the Code of Administrative Procedure, which allows the affected citizens to address an administrative authority if they believe that, in their case, an administrative authority employed an incorrect official procedure or if they object against unsuitable conduct of officials. Compared to the previous year this number increased by nine cases. Of the twenty-seven complaints, a total of three were assessed as justified and one as partly justified. Thus, compared to 2006, there was a decrease in the ratio of complaints that were evaluated as justified or partly justified. Of the total number of twenty-seven complaints, only one was aimed against unsuitable conduct of officials; after investigation, this complaint was evaluated as unjustified.



Complaints Handling and Provision of Consultations

In a vast majority of cases, the Complaints and Consultations Department, which provides services to the public on the basis of Article 29 (1) (c) and (h) of the Personal Data Protection Act, initially responded to a telephone call by the applicant; 35 questions were answered, on average, every day in 2007. A written answer or personal consultations usually followed in more complicated cases. The following cases can be mentioned as an example of 60 personal consultations provided in the relevant year to central bodies of State administration, public administration and the private sector: the Ministry of Interior, Justice, Defense, Finance and Culture; General Directorate of Customs; Police of the Czech Republic; Military Police; Inspectorate of the Municipal Police; Czech National Bank; Československá obchodní banka; Mesit holding; the companies Siemens, Bosch, Hitachi, Škoda Auto and Auto Esa; Lidl retail chain; Prague Center of Social Services; and Agricultural Water Management Administration. A total of 1 674 inquiries were handled by e-mail (1 413 in 2006).

There has been a constant increase in practically all the monitored indicators – 19 % for inquiries, 21 % for complaints; and as much as 50 % more personal consultations.

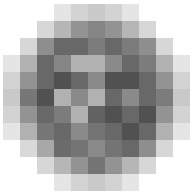
Statistical data on complaints handled in 2007

Total	574
of which:	
submitted for control	207
submitted for commencement of proceedings	35
forwarded to the competent bodies	5
suspended with notification	327

Of the total number of 574 complaints, 207 were forwarded for further analysis prior to potential commencement of control. The most common type of misconduct consisted, similar to 2006, in incorrect use of camera surveillance systems with recording equipment.

The number of complaints and inquiries newly increased in the area of processing of biometric data, specifically, in particular, in the area of fingerprints. The Office considered it necessary to adopt a fundamental standpoint on this issue right from the beginning. The use of systems whose memory stores biometric data cannot be considered to be necessary for any common records. The Office admits the possibility of using systems allowing for creation of a numerical figure through a one-way hashing function, where this figure cannot be reconstructed to obtain the original biometric data and serves only for verification of entry of an authorized person into a certain area that is, for a certain meaningful reason, protected by a special regime. However, even in this case, the data controller cannot avoid the requirement for obtaining an express written consent of the data subject to initial processing of the fingerprint and, of course, must also fulfill other duties of the data controller. Of substantial importance is particularly the information duty with-

in the meaning of Article 11 of the Personal Data Protection Act with emphasis on obtaining the consent of all affected entities; otherwise, deployment of this verification system would lose its sense.



Administrative proceedings

General part

Given the fact that, since 2006, administrative proceedings related to torts pursuant to the Personal Data Protection Act are also pursued by the inspectors of the Office, the Administrative Proceedings Department could concentrate, in 2007, also on other types of administrative proceedings that are entrusted to it (from January 1, 2007) pursuant to the organizational rules of the Office, i.e. proceedings pursuant to Article 17 (1) of the Personal Data Protection Act, which are pursued on the basis of instigations of the Registration Division. These proceedings are pursued ex officio in cases where a justified concern arises on the basis of a lodged notification of personal data processing that this processing could be at variance with the Act. Practically all these administrative proceedings pursued in 2007 were concerned with notified deployment of camera surveillance systems (37 in schools, 22 in enterprises, 8 in apartment buildings, 6 in hospitals and 6 in public administrative bodies). While most proceedings are aimed at remedying problems with fulfillment of the information duty (see Article 11) and the period of preservation of recordings (see Article 5 (1) (e)), a number of cases involve the persisting issue of excessive infringement on privacy and, therefore, processing is not permitted (with reference to violation of Article 5 (2) or Article 10 of the Personal Data Protection Act). Several penalties have already been imposed for installation of camera surveillance systems not corresponding to the requirements of the Act.

The competence of the Office newly includes misdemeanors pursuant to Section 23 (a) and (b) of Act No. 159/2006 Coll., on conflict of interests. During 2007, the Administrative Proceedings Department discussed only one such misdemeanor.

In response to frequent questions as to the manner in which the Office sets the amount of the fine, it can be stated that the basic aspects affecting the amount of the penalty consist in the criteria set forth in Article 46 (5) of the Personal Data Protection Act, i.e. the nature, gravity, manner of conduct, degree of fault, period of duration and consequences of the illegal conduct. The aforementioned aspects must always be taken into consideration. However, there are certain ambiguities related to their interpretation; thus, it can be specified that the following are involved: broader circumstances of the illegal conduct; degree of fault in the conduct (only for natural persons, because fault is, as a rule, never taken into account with respect to legal entities – "strict liability"); period of duration and scope

and character of the consequences (in summary, this could be described as the gravity of the misconduct).

In addition to these general criteria, it is also possible to specify a special group of aspects that are based on the wording of the Personal Data Protection Act:

- whether publication, disclosure, unauthorized processing or "other endangerment" of personal data is involved;
- what is the number of affected data subjects;
- whether the unauthorized processing affects sensitive data or other personal data;
- and whether human dignity has been impaired or whether the offender obtained any other benefit from the unauthorized processing.

It can be summarized on the basis of the supervisory activities of the Office that fundamental criteria include the quantity and category of personal data and the number of data subjects whose personal data were processed without authorization or, as the case may be, endangered. Thus, the number of endangered data subjects has, undoubtedly, most frequently a fundamental effect on the amount of the penalty.

Special part

Interesting penalty proceedings pursuant to the Personal Data Protection Act and the Certain Services of Information Society Act

- Performance of judicial distress

Violation of the Personal Data Protection Act has been found in activities of a person entrusted with the performance of judicial distress in relation to personal data processing of the obliged party within the distress. At variance with the Personal Data Protection Act, this distrainer specified, in the operative part of the decision on the price, which he subsequently posted on his website, the birth number of the obliged person, even though no legal regulation imposes on the judicial distrainer the duty to publish the resolution on the price in this manner.

Pursuant to Article 13 (7) of the Register of Population Act, only a natural person to whom a birth number has been assigned or his/her legal representative may use the birth number of make a decision on its use; otherwise, the birth number may be used only in the cases stipulated in Article 13c of the Register of Population Act. Pursuant to Article 13c (1) (a) of the Register of Population Act, a birth number may be used only for activities of the Ministries, other administrative authorities, bodies entrusted with the performance of State administration and courts, provided that this follows from their statutory duty, or the notaries – for the needs of keeping the Central Register of Wills. Pursuant to Article 28 of Act No. 120/2001 Coll., on judicial distrainers and distress (the Code of Distress Procedure) and on amendment to other laws, the acts of a distrainer with the performance of distress are considered to be acts performed by the court. Therefore, it can be stated that a judicial distrainer is authorized to use birth numbers in his activities. Simultaneously, it must be noted that, although administrative authorities and courts are generally authorized to use birth numbers, this provision cannot be construed in that they may use the birth number without any limitation; in its use, they must concurrently respect Article 5 (1) (f) of the Personal Data Protection Act, according to which the controller is obliged to process personal data only in accordance with the purpose for which the data were collected within the performance of his activities. Indeed, no legal regulation contemplates that a birth number should be processed for the purpose of its publication. At the same time, no legal regulation, and specifically Act No. 99/1963 Coll., the Code of Civil Pro-

cedure, stipulates that a resolution or judgment should identify the parties through their birth number.

In the mentioned case, the birth number of the obliged party was set forth in the resolution on the price of a real estate. The requisites of a resolution are stipulated in Article 169 (1) of Act No. 99/1963 Coll., according to which a resolution shall include, amongst other things, identification of the parties. In accordance with Article 167 (2) of Act No. 99/1963 Coll., the provisions on a judgment may apply to a resolution; Article 157 (1) of Act No. 99/1963 Coll. requires "exact identification of the parties". According to the last sentence of this provision, where possible, the identification of the parties shall also include their date of birth (identification number). Therefore, by logical interpretation, it can be unambiguously concluded that the requirement for specification of the date of birth, in addition to "exact identification of the parties" in a judgment (and thus also in a resolution), means that "exact identification of the parties" does not include specification of their birth number, because, in that case, specification of the date of birth of the parties to the proceedings would be entirely redundant.

Reference can also be made to the commentary on the Code of Civil Procedure (Bureš J. a kol.: Občanský soudní řád: komentář (Code of Civil Procedure: commentary), C.H. Beck, 6th edition, Prague 2003), which refers, in relation to identification of the parties in a judgment, to identification of the parties in the action; here it is stated that a natural person as a party to the proceedings must be identified by his or her name, surname and place of residence. Where this is necessary or required (the person who lodges the proposal, e.g., does not know the place of residence, or the party is not present at the place of residence; several persons with the same name and surname live at the same address, etc.), additional information must be specified (date of birth, birth number, place where the person is staying, place of business). It should be added that the birth number, as a general identifier of a natural person that is subject to special legal protection pursuant to the Register of Population Act, may be used only as a last resort; in a vast majority of cases, it will be sufficient to identify the party to the proceedings through his name, surname, place of residence and date of birth.

In accordance with the aforementioned considerations, the argument that, in distress proceedings, it is necessary or perhaps the sole option to absolutely specifically identify the obliged party through the birth number is at variance with the current legislation, inter alia, also because the requirement for identification of the party before the court is always the same, regardless to whether this is a common civil fact-finding procedure, criminal procedure or distress procedure; indeed, in the first two cases, the birth numbers of the parties are not generally stated in the judgment. Indeed, ad absurdum, it could be concluded that distress cannot be ordered on the basis of a judgment that does not contain the birth numbers of the parties, as the court would not be certain that distress will actually be ordered against the obliged party, which had the duty imposed by the judgment to provide a performance, as it was not identified in the judgment with sufficient precision.

Similarly, the authorization to use birth numbers for identification of defendants also cannot be derived from the fact that both the Land Registry, which is a public registry accessible also by remote access, and the title sheet, as a public deed, contain birth numbers and thus disclose them to the general public. Processing of birth numbers in relation to keeping the Land Registry is in conformity with Article 13c (1) (a) of the Register of Population Act. However, neither Act No. 344/1992 Coll., on the Land Registry of the Czech Republic (the Cadastral Act), nor any other legal regulation stipulates the authorization of the users of these records to freely dispose of the birth numbers set forth in the records.

With respect to publication of the resolution on the price on the website of the distrainers' authority, it can be stated that this manner of personal data processing of the obliged party is also at variance with Article 5 (1) (f) of the Personal Data Protection Act because no legal regulation imposes on the judicial distrainers the duty to publish a resolution on the price in this way. Pursuant to Article 336a (4) of Act No. 99/1963 Coll., a resolution on the price shall be delivered to the entitled party, to those who joined the proceedings as further entitled parties, to the obliged party and to persons that are known to have benefit from rights or encumbrances related to the real estate. Thus, this resolution is not further published in any manner. Consequently, in the sense of Article 2 (3) of the Constitution of the Czech Republic, pursuant to which State power may be exercised only in cases, within the limits and in manners stipulated by a law, the Office considers publication of a resolution on the price on the website of a party to the proceedings to constitute personal data processing that is not in accordance with the purpose for which the data were collected.

For the mentioned breach of the duty pursuant to Article 5 (1) (f) of the Personal Data Protection Act, the Office imposed a fine of CZK 8,000, which was confirmed by a decision of the President of the Office on the basis of an appeal; this decision was subsequently challenged by an administrative action.

■ Enforcement of receivables

Another fine for violation of the Personal Data Protection Act was imposed (in two separate proceedings) on two persons who stated in a press release related to enforcement of receivables of a business company that receivables had been enforced from a natural person (stating the name, surname and maiden name), including specification of the debt, the competent court and the file number of the case and date of payment of the amount. Through the mentioned conduct, these persons breached the duty stipulated 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.

Publication of personal data is one of the manners of processing within the meaning of Article 4 (e) of the Personal Data Protection Act. While it is stated in an amendment to the mandate contract, on the basis of which the parties performed their activity, that the information provided to them by the business company for the purposes of enforcement of receivables is in no case subject to the regime of the Personal Data Protection Act, the Act also contains mandatory provisions of public law, whose application cannot be excluded by the parties by agreement, which would thus evade the duty following from it.

The business company collects personal data of persons from whom it has a receivable and is the controller of these personal data. To this end, it also performs further personal data processing of these persons, e.g. maintains, sorts or transfers these personal data. The parties to the proceedings concluded a mandate agreement with the business company and, on its basis, they enforced its receivables from these persons, who had failed to pay their debts duly and in time, even after they were requested to pay the debts in relation to this finding. Therefore, on the basis of the authorization in the agreement, the parties to the proceedings processed personal data of persons against whom they enforced the receivables.

In the given case, it is clear that these parties processed these personal data within the meaning of Article 4 (e) of the Personal Data Protection Act, as they, e.g., used, transferred, maintained or sorted these personal data. At the same time, the second condition stipulated in the definition of processing, i.e. the requirement that the aforementioned operations with personal data be carried out systematically, was also fulfilled. The criterion of systematic processing is fulfilled with

respect to the fact that one of operations characterizing the processing is carried out with a certain objective. In this case, the systematic nature is based on the actual manner in which the personal data were kept by the business company and submitted to the parties to the proceedings, where a joint computer network was used. Furthermore, it can be stated that the parties to the proceedings agreed in the mandate agreement that they would keep the records of all the assumed receivables, both in the form of documents and in the form of computer documentation (keeping records of receivables undoubtedly corresponds to the term maintenance in the definition of processing), where the most important element of keeping any documentation is its systematic nature.

The business company processed personal data of a natural person for the purpose of enforcing its receivables, where it entrusted the parties to the proceedings, in the mandate agreement, with processing these personal data for the same purpose. Pursuant to Article 5 (1) (f) of the Personal Data Protection Act, i.e. the data controller (or processor) is obliged to process personal data only in accordance with the purpose for which they were collected. Nevertheless, the parties processed personal data of a natural person also after the outstanding amount has been paid, where they selected from the overall records of receivables only those that concerned this natural person and then published them in the press release; however, publication constitutes one of the manners of processing within the meaning of Article 4 (e) of the Personal Data Protection Act. This processing of personal data does not correspond to any of the purposes for which the parties to the proceedings were authorized to process personal data of the debtors on the basis of the mandate agreement. At the same time, it can be stated that it also does not correspond to the purpose for which the business company processes personal data. For breach of the duty set forth in Article 5 (1) (f) of the Personal Data Protection Act, the Office imposed a fine in the amount of CZK 25,000 on each of the parties to the proceedings. As in the previous case, these fines were challenged by an administrative action.

■ Sending of commercial communications

Violation of the Act was found in the case of a business company that sent commercial communications without demonstrable consent of the addressees, whereby it breached the duty stipulated in Article 7 (2) of the Certain Services of Information Society Act, according to which details of an electronic contact can be used for the purpose of disseminating commercial communications by electronic means only in relation to those users who have previously granted their consent to this effect.

On the basis of the agreement on provision of information services of the European Databank, the business company was a participant in the European Databank and claimed that it had the authorization to send commercial communications to the other participants in this database on the basis of the agreement. On the contrary, the companies contributing to the administration and operation of the database, i.e. the provision of its services, stated that it was not true that all the participants in the database of the European Databank were aware that, on the basis of inclusion in the database, they could be addressees of commercial communications sent by other entities in the database, as they could only be addressees of demands for their products or services. Furthermore, they stated that the general terms and conditions of agreements on provision of information services of the European Databank, concluded with the participants in the database, do not contain the consent of the participants to the fact that their electronic address should serve for mutual communication amongst the participants in the database.

According to the aforementioned agreement, the consent of the party to the proceedings to its inclusion in the database of the European Databank was granted for the purpose of publication and provision of information through the provider for the purposes of promotion of activities, advertising and marketing purposes and in order to be able to send demands for the thus-presented goods or services, rather than for dissemination of one's own promotional materials; therefore, this was clearly not a consent to dissemination of commercial communications by electronic means.

On the website of the European Databank, every participant is automatically provided with his own website, which contains a note that a message of the participant (demand) will be delivered indirectly and that it will not be delivered if it has the character of an offer.

The first-instance body of the Office imposed a fine of CZK 10,000 for breach of Article 7 (2) of the Certain Services of Information Society Act. Based on an appeal, the President of the Office cancelled the contested decision within appellate proceedings and returned the case to the first-instance administrative body for new discussion. The first-instance body supplemented the file on the basis of the conclusions contained in the justification of the second-instance decision and imposed a fine in the original amount, which was confirmed by the President of the Office on the basis of a new appeal.

■ Decisions of the Office on misdemeanors pursuant to the Act on Conflict of Interests

The conduct of the accused person consisted in publication of data from property reports of the members of the Government in one of the Czech daily newspapers; however, the author did not deal with any specific case of conflict of interests with respect to any of the persons whose data were published. The article dealt solely with control of property reports submitted by Czech politicians, i.e. summarized the contents of the information on assets and liabilities, as presented by the mentioned politicians in their notifications submitted pursuant to the Act on Conflict of Interests. However, this Act stipulates that all data kept in the register may be used and further processed only for the purpose of ascertaining a potential conflict of interests in the performance of duties of a public officer; by breaching this duty, a natural person commits a misdemeanor.

The Office came to the conclusion that the actual publication of the data from the register, without being connected with some other fact or information that could or should lead to ascertaining a potential conflict of interests, does not fulfill the condition of authorized use of the data. Based on this consideration, it came to the conclusion that, through his conduct, the accused person committed, from the formal viewpoint, a misdemeanor pursuant to Article 23 (a) of the Act on Conflict of Interests, as he used the data for a purpose other than ascertaining a potential conflict of interests.

However, simultaneously, the Office dealt with the aspect of the material element of the conduct, i.e. with the question as to whether the conduct of the accused can be considered to be conduct breaching or threatening an interest of society. If this element is not present, the given conduct cannot be considered to be a misdemeanor.

The Act on Conflict of Interests contains a very broad definition of public officers; amongst them, it includes persons from members of the Government, Deputies and Senators, senior governmental officials, judges and members of municipal and regional assemblies, to police officers and normal senior public servants. The rules for management of their personal data in the register of processing are defined in the same manner for all these persons, even though it is clear that they play very

different roles in society from the viewpoint of their position. In the given case, it is clear that also the degree of protection of their privacy and private life must be assessed differently. In this relation, in accordance with the case-law of the Constitutional Court and the European Court for Human Rights, the Office considers that it is necessary to create a certain hierarchy of publicly active persons; members of the Government are at the top, followed by line politicians at the national or local level, other publicly active persons, such as celebrities, as well as officers, judges, attorneys-at-law, and ending with normal citizens that do not hold any position or play an important role in society.

In this relation, the Office also assessed the conflict of the constitutional right to protection of privacy (Art. 10 of the Charter of Fundamental Rights and Freedoms and Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms) and the right to freedom of speech (Art. 17 of the Charter of Fundamental Rights and Freedoms and Art. 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms). As follows from the limitation of the manner of use of the data obtained from the register of notifications in the Act on Conflict of Interests, the legislature stipulated the rules on access to and use of information from the register with the aim of striking balance between these two constitutional rights. The statutory limitation thus allows for fulfillment of the objective of this Act, i.e. ascertaining and preventing conflicts of interests, while simultaneously avoiding substantial infringement on privacy of the obliged persons (public officers), i.e. uncontrolled management of data on their property. However, simultaneously, the Act in no way takes account of the different roles of these persons as "public personages".

Nevertheless, or maybe exactly for this reason, the Office believes that, in the case of members of the Government, i.e. persons standing at the top of the executive power, it may be concluded, through interpretation conforming to the Constitution, that mere publication of information on their property in a newspaper does not infringe or threaten an interest of society. It is clear that members of the Government have considerable powers to make decisions on the most important issues involving public expenditures, internal and foreign policies of the Czech Republic, etc. This power undoubtedly gives rise to greater public interest in transparency and control of their decision-making, inter alia, from the viewpoint of possible conflict of interests. At the same time, the Office notes that it is necessary to take into account the fact that one of the tasks of the press in free and democratic society is to play the role of a "public watchdog".

Imposed penalties

In this part, we concentrate on three most important cases of breach of duties in personal data processing – based on the amount of imposed penalty.
N.B. : Only proceedings on administrative torts that were validly completed in 2007 were included in this part.

One of the highest fines in the past year was imposed on a ministry that, as the data controller, processed personal data of persons deceased before 1956 in relation to maintenance of the Information System for Register of Population (ISRP), although, pursuant to Article 9 (1) of the Register of Population Act, this period is stipulated at 50 years from death of the person or the person being declared dead, and also created auxiliary data items (personal data) that are not included in the exhaustive list stipulated for this information system by the law and allowed their disclosure to the recipients of data from the ISRP. It also violated the Act by failing to provide data subjects with the required information and instruction on their rights related to personal data processing and allowing operations, particu-

larly testing for developmental purposes, using "hard" data, which represented an increased risk of unauthorized processing, change or even loss of personal data in the ISRP, based only on informal security measures consisting in an oral or implicit instruction of the authorized employees. Through the above-described conduct, the ministry breached Article 5 (1) (e) and (f), Article 11 (1) and (2) and Article 13 (1) of the Personal Data Protection Act, for which the Office imposed a fine, through an order, in the amount of CZK 1,000,000. On the basis of a protest, it was acknowledged that the performance of the duties in the personal data processing in ISRP is stipulated in several legal regulations that must be complied with simultaneously and also that it had not been proved that the right to protection of personal data or the right to protection of private and family life would be infringed. Therefore, a fine equal to CZK 400,000 was ultimately imposed through a final decision. The decision has been challenged by an administrative action which is still pending.

Another penalty was imposed by the Office on a trade union that, in relation to the operation of a camera surveillance system installed in the offices of the chairman and the secretariat, collected personal data of all persons who were present on these premises during the working hours in the second half of 2004, without having obtained their consent to personal data processing, although the given processing was not subject to any of the exemptions permitting personal data processing without consent of the data subjects. Furthermore, it breached the duty to inform the data subjects of the conditions of this processing, i.e. the scope in which and the purpose for which the personal data would be collected, who and in what manner would process the personal data and to whom the personal data could be disclosed; it also failed to inform them of their right of access to personal data and the right to have their personal data rectified, as well as other rights stipulated in Article 21 of the Personal Data Protection Act. Simultaneously, it failed fulfill another duty, which requires the adoption of measures preventing unauthorized or accidental access to personal data, their change, destruction or loss, unauthorized transfer and other unauthorized processing. As a consequence of these failures, a hard disk containing recordings from the camera surveillance system was stolen from a personal computer and these recordings were subsequently published in television broadcasting. Thus, the aforementioned conduct led to breach of Article 5 (2), Article 11 (1) and Article 13 (1) of the Personal Data Protection Act, for which the Office imposed, through an order, a fine on the trade union in the amount of CZK 200,000. Following a protest, a penalty in the same amount was imposed on the trade union also by the first-instance decision, which was later confirmed by a decision of the President of the Office. Similar to the previous cases, this decision has been contested by an administrative action.

In the performance of the power to impose penalties pursuant to the Personal Data Protection Act, the Office imposed, during the last year, a fine also on a company providing electronic communication services; through its dealer, who was in the position of a data processor, this company concluded agreements on connection and provision of public retransmission services and on purchase and sale. Each this agreement was accompanied by a copy of the identity card, which the contracting partner was obliged to request upon conclusion of agreements; this obligation was stipulated in an annex to the mandate contract. Furthermore, some agreements also included attachments containing a copy of the passport or driving license, and also a copy of the bank payment schedule SIPO, which were gathered by the given processor entirely beyond the scope of his obligations. This led to collection of redundant personal data obtained from the copies of both sides of identity cards, including the family status, maiden surname, place of birth, information obtained from the photograph and, where stated, the name, surname and

birth number of the spouse and children. This also led to breach of several provisions of the Personal Data Protection Act. This included, in particular, collection of personal data by the company at variance with the set purpose and within a scope that was not necessary for fulfillment of this purpose, i.e. conclusion and performance of contracts, for which the Act on Electronic Communications stipulates an exhaustive lists of requisites. Thus, in the opinion of the Office, in accordance with the applicable provisions of the special legal regulations, it is sufficient for identification of a party to a contract on lending and borrowing to state the name, surname, address and date of birth of a natural person. Furthermore, the company did not fully perform its information obligation in that it failed to inform its clients of their right of access to personal data, the right to have the personal data rectified and other rights stipulated in Article 21 of the Personal Data Protection Act. It also failed to transfer this obligation to its processors and it also did not inform the clients on whether the provision of personal data is obligatory or voluntary. Thus, the aforementioned conduct led to breach of Article 5 (1) (d) and Article 11 (1) and (2) of the Personal Data Protection Act, for which the company received a fine of CZK 57,000.

Number of instigations and proceedings held:

Number of instigations related to penalty proceedings pursuant to the Personal Data Protection Act, Register of Population Act, Act on Conflict of Interests and Certain Services of Information Society Act

total ----------2

of which

– on the basis of an instigation from natural and legal persons -----41

– on the basis of referral by the prosecuting bodies and bodies dealing with misdemeanors ----------25

– on the basis of control activities of the Office ----------16

Handled: (including handling of instigations, whose discussion was commenced in 2006)

– through discontinuation prior to commencement of proceedings, referral to the competent body ----------21

– through a decision on imposing a penalty (total) ----------43

– of which with legal force ----------32

– discontinuation of proceedings, decision that a tort has not been committed ----------18

Number of instigations in case of justified doubts as to the lawfulness of the notified processing (proceedings pursuant to Article 17 (1) of the Personal Data Protection Act)

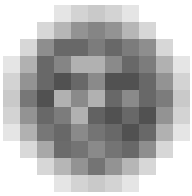
Total ---------- 115

Handled:

by not permitting processing ---------- 16

by discontinuing proceedings (the data controller does not breach the conditions stipulated by the Act) ---------- 76

by discontinuing proceedings (personal data are not processed)------ 4



Legislation in 2007

Schengen Amendment to the Personal Data Protection Act

This amendment to the Personal Data Protection Act was one of the key parts of Schengen acquis implementation and its adoption became a necessary step for accession of the Czech Republic to the Schengen area. The amendment to the Act was discussed, together with amendments to further regulations, as a single amending law, without any comments and modifications by the Parliament (see parliamentary press No. 187) and published under No. 170/2007 Coll.

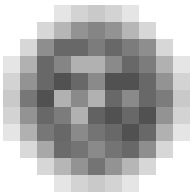
In this relation, the Office welcomed the recommendation of experts within the performed evaluation of preparedness of the Czech Republic for accession to the Schengen area; however, at the same time, when creating the amendment to the Act, it considered the current documents and the ensuing requirements so as to ensure that the formulated rules are not at variance with the almost completed draft documents for the new version of the Schengen Information System (SIS II). This was then reflected in the following areas: 1. the supervisory competence of the Office was further specified (Article 2 (2) and (3), Article 29); 2. the group of biometric data included amongst sensitive data was more accurately defined (Article 4 (b)); 3. minor changes were made in the area of processing of sensitive data (Article 9); and 4. the rules concerning security of personal data were further elaborated (Article 13 (3) and (4)). For the sake of completeness, it should be added that, beyond the scope of the Personal Data Protection Act, expert recommendations were incorporated with greater or smaller success, in special regulations concerning, in particular, the police and customs administration, e.g. in the area of access of citizens to data maintained about them, the right to have these data rectified and the duties of the authorities and security corps to provide information about processing of these data.

In the area of external legislation, in the past year, the Office expressed its opinions most frequently on legislative drafts and the related materials of a non-legislative nature, concerning e-government. In this relation, the Office repeatedly noted that new electronic records and communication flows cannot be simply regulated in the legislation and, de facto, arise through mere copying of the rules for manual or partly automated form of data processing. From the viewpoint of personal data protection, electronic communications can introduce more efficient personal data treatment; however, at the same time, they require stricter conditions, particularly for securing the records and personal data transfers. However, the laws often do not contain these conditions, usually based on the requirement that legal regulations should not be dependent on a specific technology. The revision of the basic registers of the State administration that is planned for 2008 and which should also encompass elaboration of the principles of personal data processing (e.g. in maintenance of data, but also in the area of access of citizens to their data, as has already been indicated in the CzechPoint project) will be an actual basis for electronic communication and e-government.

Negative cases where the party submitting a draft legal regulation was not willing to have the draft wording evaluated from the viewpoint of privacy and personal data protection occurred again in 2007. This was the case, e.g., with respect to the amendment concerning speed measurement on roads, which was proposed without discussion with the Office after agreement of ministers (!) through MPs' initiative (!). It is not clear why no time had been found for minor modifications and potential supplementation of the explanatory notes by a more detailed description of the manner of handling the records of measurement of speed (see parliamentary press No. 185); these modifications and supplementations were necessary from the viewpoint of citizens' privacy protection.

The draft new Act on the Police of the Czech Republic is a case that would deserve more careful preparation of the statutory rules for personal data processing. In this case, the Office would welcome if it were notified of the draft comprehensive regulation of special personal data processing sufficiently in advance and if it were able to express its opinion on this issue, e.g. within the relevant expert groups. Indeed, within the commentary procedure, it is difficult to discuss and change the structure of the proposed law.

The 2007 amendment to the Act on Care of Peoples' Health, which was supported by the Office from the beginning, can be considered to be a case appropriately reflecting the rules for personal data processing. Negotiations with ministries that recently proposed modifications (from the viewpoint of the Office, often redundant) of personal data processing were also beneficial. Negotiations have already been completed with the Ministry of Education, Youth and Sports, whose representatives have been provided with the opportunity to become acquainted with the rules of protection of privacy and the rather differing opinion of the Office on centralized keeping of data from citizens at a time when the State delegates an increasing number of specific tasks to municipalities and other entities by means of public-law regulations.



Schengen cooperation

1. PREPARATION AND EVALUATION

Evaluation of preparedness of the Czech Republic for adoption of the Schengen regulations in the area of personal data protection, including functional control performed by an independent supervisory authority and application of the data protection standards in the practice of all the ministries involved culminated in the visit of the expert mission in March 2006. The final phase of evaluation took place at the end of September 2007, including review of the conditions of the Schengen Information System (SIS) operation, which was put into operation already on September 1, 2007 for the reason of the necessary technical preparations in the Czech Republic.

Given the fact that the Czech Republic was, more or less, positively assessed in all areas and the potential shortcomings were gradually resolved within the "follow-up" process, on November 8, the meeting of the EU Council for Justice and Home Affairs confirmed preparedness of the Czech Republic and 8 other EU countries for abandoning national borders as of December 21, 2007 for internal land and marine borders, and as of March 30, 2008, at international airports for flights inside the Schengen area. The final decision on the Schengen area enlargement was then adopted at the Council meeting on December 6 and 7, 2007.

2. COMPETENCE OF THE OFFICE IN RELATION TO SIS AND RELATED ISSUES

The Schengen Information System as a compensation for removal of border controls consists, in fact, in a joint database shared by all Member States, which contains a great many various pieces of information, including personal data. Processing of data included in the system is governed by strict rules for personal data protection, which are formulated both in the Convention implementing the Schengen Agreement (international agreement of 1985, which created, inter alia, the SIS) and in the national legislation on data protection in the individual Member States.

The task of the Office in the area of Schengen cooperation is to supervise over the adherence to the principles of protection of personal data processed particularly within the SIS (and also in other forms of cooperation of the competent authorities) and guarantee of the rights of persons to whom the processed data are related.

The competence of the Office also includes supervision over due personal data processing in other supranational information systems, which are usually related in a certain way to the Schengen cooperation, or cooperation within the EU 3rd pillar (cooperation in the area of police and justice, i.e. aspects that are not governed by the Community principle of majority, but are rather left to sovereign decision-making by the Member States), such as the Visa Information System (VIS), Customs Information System (CIS) and the EURODAC system for comparison of fingerprints of asylum applicants.

The second generation Schengen Information System (SIS II) is also being developed at the present time; from 2009, this system should replace the current SIS and will contain biometric data (photographs, fingerprints) and allow for sharing and use of entries by a greater number of entities.

The fundamental rights of the data subjects in relation to the SIS include, in particular, the right to be informed of the data related to the data subject, the right to have incorrect data rectified or the right to request deletion of the data entered in the system without authorization. An integral part of this right also consists in the option to address, in any Member State, the national supervisory body for personal data protection with the requirement for verification of data processing in the SIS. Furthermore, the right to bring a matter to courts or some other competent authority and claim correction or deletion of the data kept in the SIS or request the provision of information or, as the case may be, indemnification, is also guaranteed.

3. SCHENGEN COOPERATION AND THE 3RD PILLAR DEPARTMENT

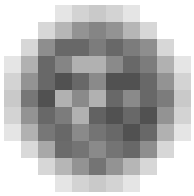
In order to fulfill all the tasks following from the new competencies of the Office in the area of the Schengen cooperation, as well as within the aforementioned related agenda, a new department of the Office was established as of July 1, 2007 – the Schengen Cooperation and the 3rd Pillar Department (hereinafter the "Department").

The basic activities of the Department include acceptance and handling of instigations and complaints from citizens in relation to unauthorized processing of data in the SIS and answering questions concerning personal data processing within this system. Particularly through analyses of the received instigations and the ensuing strategic activities, the Department will also be involved in the supervision over personal data processing within the national part of the Schengen Information System. If it is found that the duties in processing of personal data within the SIS have been breached by the Czech authorities, the Department will pursue proceedings on administrative torts that can result in imposing a penalty (fine).

An important part of the work of the Department consists in the provision of information about the conditions of personal data processing within the SIS to the general public, which is ensured particularly through the Bulletin, Journal of the Office, and the "Schengen" section of the Office's website.

The working tasks of the Department also include cooperation with other sectors that contribute to personal data processing within the SIS in the Czech Republic. This involves primarily consultancy and, if appropriate, participation in the creation of the necessary legislative measures (such as Act No. 170/2007 Coll., amending some laws in relation to accession of the Czech Republic to the Schengen area) or implementation of joint information campaigns.

The Department closely cooperates with similar foreign supervisory authorities and also provides for participation of the Office in the meetings of the Joint Supervisory Authority (JSA Schengen) and other bodies or working groups, both national and foreign, concentrating on the related topics (e.g. Visa&Biometrics, EURODAC, JSA Customs or the working group for the SIS II information campaign).



Registration Activity

The Registration Department provides for keeping of the register of personal data processing which consists particularly in acceptance of registration notifications, their review and keeping records of these notifications, and also deals with issues related to personal data transfers abroad.

Consultancy became an important part of the work of the Registration Department in 2007, as the data controllers increasingly addressed the Department with requests for consultancy before they actually submitted a written notification on data processing. The entire registration process was further specified and improved in 2007 due to the introduction of the electronic registration forms.

REGISTRATION PROCESS

The register of data processing kept on the basis of Article 29 (1) (b) of the Personal Data Protection Act allows everyone to learn, at any time, who processes his personal data, where and to what extent, and under what conditions. Therefore, the register is publicly accessible, also by remote access through the Office's website. Entry in the register or registration certificate issued by the Office at the notifier's request continues to be incorrectly considered by a number of data controllers to be a proof of the fact that the Office has permitted the processing. However, a registration certificate issued by the Office merely documents that the controller has fulfilled his statutory obligation to notify the Office in advance of intended processing and that the processing has been recorded in the register by the Office.

A different situation occurs in the event that a justified concern arises, on the basis of the notified processing, that the laws could be violated in the processing of personal data. In that case, the Office is obliged to initiate proceedings ex officio pursuant to Article 17 of the Act, which de facto fulfills the needs and objective of prior checking within the meaning of Article 20 of the Directive. These proceedings proved to be very effective in assessing the intention to deploy camera surveillance systems (see also the chapter Administrative proceedings – general part).

PERSONAL DATA PROCESSING THROUGH CAMERA SURVEILLANCE SYSTEMS

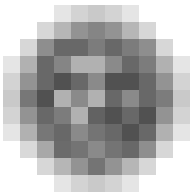
The number of data controllers who notified the intention to operate camera surveillance systems doubled in 2007, compared to the previous year and a similar increase occurred in relation to the number of inquiries and consultations related to the conditions of installation of camera surveillance systems. (While only 5 controllers operating camera surveillance systems notified in 2005, their number increased to 380 in 2006 and to 790 in 2006.)

One of the main notified purposes of cameras installations consists in property protection. It should be emphasized in relation to installation and operation of camera surveillance systems that protection of property may not be generally preferred to protection of privacy, which is often the case.

The Office came to the conclusion that, in a number of cases, camera surveillance can be easily avoided and replaced by some other, less invasive, but similarly effective, technical means.

Another alleged objective of a camera surveillance system installation consists in health and life protection; however, a camera recording can hardly serve this purpose and, thus, in this case, its installation is unsuitable for attainment of the purpose declared by the controller.

The principle of purpose (finality) of personal data processing is further developed in labor-law relations in Article 316 (2) and (3) of the Labor Code, which prohibits monitoring of employees by cameras, unless there is a serious reason related to the special nature of the employer's activities. It is often very difficult to set the degree of the reasons importance in relation to the special nature of the employer's activities and to express why this activity is so special for it to be possible to infringe on the employees' privacy. Nevertheless, it is necessary to strictly disagree with the efforts of certain employers to commence the operation of camera surveillance on the premises of their company in order to prevent minor disciplinary misconduct, such as prevention of smoking or disorder in the canteen, enforcement of use of safety means, etc.



Transfer of Personal Data Abroad

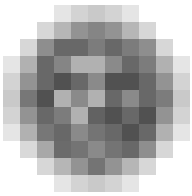
The most important events that related to the subject of personal data transfers to third countries in 2007 were connected with air transport. The Office received several applications from the Czech Airlines that were concerned with submission of very detailed data on their clients (passengers), and also their employees (crews of aircraft), to the competent authorities in final destinations (Kuwait, Cuba, etc.), which intended to use them to check the individual passengers before they boarded the aircraft.

A new agreement between the European Union and the United States of America on processing passenger name records (PNR) by air carriers and their submission to the Department of Homeland Security of the United States of America was concluded in July 2007. However, the Office considers the agreement to be inadequate from the viewpoint of guarantees of the level of personal data protection. Indeed, the provided guarantees are even smaller than those contained in the previous agreement of October 2006, although even the latter did not fully correspond to the requirements and criteria set by Directive of the European Parliament and of the Council 95/46/EC, or by Convention of the Council of Europe No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. From the viewpoint of the Office, according to this agreement, data may be processed for insufficiently defined purposes, they may be disclosed to an excessively broad and insufficiently defined range of institutions and persons, they may be maintained for an inappropriately long period of time and, in exceptional cases, sensitive data on the individual passengers may be transferred.

Two sets of Binding Corporate Rules (BCR) were submitted to the Office for comments in 2007 by the companies Akzo Nobel NV and Accenture Ltd.; these rules were recommended by the Office for approval. However, the Office stated that approval of BCR contained in its standpoint did not exclude the duty of the branches of the companies established in the Czech Republic to apply to the Office for a permit to transfer personal data to third countries within the meaning of Article 27 of the Act, in which case it would be repeatedly, and this time not only generally, examined whether the BCR, in the version for the Czech Republic, fulfill the conditions imposed by Article 27 (3) (b) of the Act for safe transfer of personal data to third countries.

The employees of the Office for Personal Data Protection have frequently been recently asked whether a parent company in the United States of America may require that the employees of its subsidiaries in Europe comply with the Act which is known as "Sarbanes-Oxley Act" (hereinafter "SOX Act"), which applies in the territory of the United States of America and which provides for notification of suspected violation of legal regulations in the area of accounting, internal accounting controls and audit issues. Application of the SOX Act to European subsidiaries (branches) of U.S. companies (and to European companies listed in U.S. stock exchanges) is currently being examined by the courts in the U.S.A. itself.

It has not always been easy to find an unambiguous answer to the question as to whether, in cases where the employees of these parent companies perform the duty following from the SOX Act and report a suspicion of potentially illegal conduct (suspicion of financial or accounting fraud), or submit the obtained proof, such a report constitutes a transfer of personal data abroad, as the persons raising this question were often not fully aware how this report of suspected potential illegal conduct would occur in practice. The Office's opinion is identical with that of WP 29 of February 1, 2006 in the sense that, if this information is submitted to the United States of America by a subsidiary and this is a permanent and systematic activity, it is most likely that a transfer of personal data would be involved. The idea that any employee could report his suspicion of potential illegal conduct to the parent company in the United States of America, without knowledge of his employer, and probably by e-mail or via a special telephone line, is absolutely at variance with the SOX Act, Directive 95/46/EC and the aforementioned opinion of WP 29 of February 1, 2006.



International relations and cooperation

The most important working platform for relations and cooperation with both the European Commission and the partner supervisory bodies in other EU countries, consisted again, during the previous year, in the Data Protection Working Party (WP29) established under Article 29 of Directive 95/46/EC. A total of 5 meetings of WP 29 took place in 2007. The most important discussed documents and ideas again included the "Proposal for a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters". In the long term, the working party has dealt with topics related to transfer of personal data to "third countries", particularly (but not exclusively) to the U.S.A., and especially the long existing problem of transfers of personal data from the passenger name records in the systems of air carriers (PNR data). Other topics included continuation of the "SWIFT case"; unification of interpretation of the definition of personal data; preparation of a material on children and privacy; proposal for alternative standard contractual clauses for transfers of personal data to "third countries"; and improvement of implementation of Directive 95/46/EC, etc.

WP 29 also has a number of working subgroups, where the Office is represented by its experts in some of them. The Office participates in activities of the Internet Task Force and subgroups for visa and biometrics, for RFID technology, for justice, freedom and security and for identity management and e-Government.

In addition to the WP 29 platform, an opportunity to pursue close relations and ensure joint handling of issues of the Office with the competent workplace for data protection (C-5 Unit) of DG Justice, Freedom and Security of the European Commission is also provided by participation in the meetings of the Committee on the Protection of Individuals with regard to the Processing of Personal Data (Article 31 Committee) established by Article 31 of Directive 95/46/EC. This is more a political body with prevailing representation of governmental agencies of the individual countries.

The Working Party on Data Protection (G09) of the EU Council is a clearly political body. The Czech Republic has been represented by an employee of the Permanent Representation of the Czech Republic to the European Union and a representative of the Office actively participated in two meetings as an invited expert.

However, the Office also cooperates indirectly with the bodies of the EU Council / Coreper, within an intersectoral cooperation in the Czech Republic. Favorably evaluated should be particularly the cooperation with the Ministry of Informatics of the Czech Republic, prior to its disestablishment as of June 1, 2007, in broad matters concerning development of the information society ("e-Europe", "e-Government", etc.), aspects of security of data and electronic communications, regulation or deregulation of services related to public communication networks, etc. The effort has been ongoing to find a manner of cooperation with the Ministry of Industry and Trade and of the Ministry of Interior, which both have taken over this subject.

The position of the Office is sometimes requested by the Ministry of Interior of the Czech Republic within creation of instructions for discussions of the Council/Coreper bodies with respect to issues of security affecting protection of data and privacy. However, the cooperation could be more systematic and it is usually difficult to enforce the opinions of the Office given the differing opinions of the two institutions with respect to a number of aspects within search for a balanced approach to strengthening security while simultaneously respecting the rights of individuals, including the right to privacy and to adequate protection of personal data. On the contrary, the Office highly appreciates the cooperation with the Ministry of Interior of the Czech Republic in the preparation for accession to the Schengen Agreement.

Certain promise for the future constitutes the preparation for the Czech Presidency in the EU Council (CZ PRES), particularly participation of the Office in the work of the "Intersectoral Expert Group for Elaboration of Priorities of CZ PRES in the Areas of Justice and Home Affairs". In this respect, at least a note on the importance of protection of personal data in relation to the priority of development of the area of freedom, security and law with its motto "Europe without Barriers" has been incorporated in the first materials of the sectoral agenda. On the contrary, in the formulation of the overall priorities of the Czech Republic for the Presidency, on a general level exceeding sectoral agenda, the Office has not been successful to date in its efforts to enforce the concept of protection of data and privacy as a cross-cutting topic, which affects, to a greater or lesser degree, a majority of tasks and handling in the administrative or legal area. Therefore, the President of the Office has sent a personal letter to the Deputy Prime Minister of the Government for European Affairs. Given the positive response, we are awaiting the first results next year, in the course of elaboration of the priorities.

An extraordinarily active cooperation is being pursued in the framework of the EU 3rd pillar with the Joint Supervisory Body of Europol – JSB Europol. A representative of the Office, inspector Ms. Miroslava Matoušová, as the Vice-Chairwoman of this body, again acted as the coordinator of the control team which carried out a regular control of personal data processing by Europol at the seat of this body in March 2007. Simultaneously, in the same position, the inspector, Ms. Matoušová, participated in the control of the central part of the Customs Information System – the 3rd Pillar at the seat of OLAF. The reports from the two controls were approved by the relevant joint supervisory bodies: JSA Customs and JSB Europol. Four meetings of JSB Europol took place during the year as well as well as three meetings of the Europol Appeals Committee, which discusses and handles complaints from data subjects.

The same inspector of the Office was invited to the control team of the inspectorate of the Joint Supervisory Body of Eurojust, which took place in November 2007 at the seat of EUROJUST. Important positions of the Office within the 3rd pillar also include participation in the Working Party on Police and Justice established by the Conference of the European Data Protection Authorities, which organizes its annual spring meetings.

A specific example of development of bilateral contacts within the EU consists in the cooperation with the partner Polish authority within the Leonardo da Vinci program. In the framework of the program, the Polish Bureau of the Inspector General for the Protection of Personal Data was granted a so-called mobility project, which generally involves projects providing the participants with the opportunity to obtain professional working experience abroad. In addition to our Office, the partners included similar authorities in France, Ireland, Germany and United Kingdom. According to the agreement, our Polish colleagues should come to Prague for three weekly stays (November 2007, January 2008, March 2008). The first stay took place

on November 22 to 29, 2007, when our Office was visited by the press officer of the Polish authority.

The EU project "Support to the Data Protection Commission of Bosnia and Herzegovina" within the CARDS Program aimed at stabilizing the situation in the countries of western Balkan was successfully completed on March 31. The project evidently obtained positive response in the beneficiary country and an unofficial request has also been made for a follow-up cooperation. The project proved that the Czech Office belongs amongst top European institutions in the area of personal data protection and that it is able to further disseminate its experience.

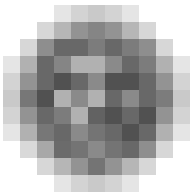
The Office received the "Prize to Data Protection Best Practices in European Public Services" awarded by the Data Protection Agency of the Community of Madrid. The winning project was selected by the international jury from over 20 nominations and was awarded on December 11, 2007 at a ceremony in Madrid. The Office was nominated for the prize by the Iuridicum Remedium association for the project of a competition for children and youth entitled "My privacy! Don't look, don't poke about!" and for the project "Protection of Personal Data in Education", which was accredited by the Ministry of Education, Youth and Sports for a period of three years within ongoing education of teachers (see also the chapter Office, Media and Means of Communication).

The Office continues to participate in activities following from the obligations of the Czech Republic as a member state of the Council of Europe and OECD. For a number of years, the Office was represented in the project group on data protection (CJ-PD) of the Council of Europe and was also an elected member of the coordination committee (CJ-PD/CG). The Office continued to actively participate in the Data Protection Committee established pursuant to Convention No. 108 (T-PD), where the Office is represented in the steering bureau by Ms. Hana Štěpánková, the spokeswoman of the Office. Based on authorization by the mentioned body, H. Štěpánková made a presentation on the European principles of personal data protection in Tirana (Albania is preparing a law on personal data protection) and in Geneva at a conference of the Asia-Europe group established by UNHCR with respect to the issue of migrants and refugees in the given region.

An exhibition of works of Czech children that were sent to the competition "My privacy! Don't look, don't poke about!" announced by the Czech Office in 2007 will be held in the Palace of Europe, the seat of the Council of Europe, in 2008 at the occasion of the Data Protection Day; the educational series entitled "Ignorance does not excuse, or Every one has secrets", which was recorded in cooperation between the Office and the Czech Television, will also be presented at this place.

In the framework of OECD, cooperation is continuing with the Working Party for Information Security and Privacy (WPISP under the ICCP committee).

In addition to the aforementioned activities, the experts of the Office participated in a number of ad hoc and regular events, such as conferences, workshops and meetings of various types



The Office, Media and Means of Communication

An extraordinary event for the Office consisted in the awarding of the Prize to Data Protection Best Practices in European Public Services. This prize was awarded to the Czech Office by the Data Protection Agency of the Community of Madrid for the project aimed at increasing awareness of personal data protection – specifically for the competition for children and youth entitled competition "My privacy! Don't look, don't poke about!", which the Office announced at the occasion of the Data Protection Day in 2007, and for the project Personal Data Protection in Education, for which the Office obtained a three-year accreditation from the Ministry of Education, Youth and Sports within DVPP (ongoing education of pedagogic workers). The Office obtained the prize in international competition of 15 projects and received it on December 11, 2007 in Madrid.

The results of the competition were also specially acknowledged by the Council of Europe in Strasbourg, where the works of the children presented within the mentioned competition will be exhibited from January 28, 2008, i.e. the Data Protection Day.

The annual report for 2007 is illustrated by reproductions of the children's works in the competition.

The competition for children and young people aged 7-18 announced by the Office for Personal Data Protection to mark Data Protection Day declared by the Council of Europe on 28 January attracted 233 contributions – essays, drawings, collages and photos. A lot of them will be exposed at the International Film Festival for Children and Youth in Zlín from 1 June 2008. Competition's winners will be ceremonially announced at the International Film Festival for Children and Youth in Zlín on 3 June 2008 at 12.00 in ZOO Lešná.

DESCRIPTION OF EDUCATIONAL PROGRAM

1. Contents – detailed survey of topics:

One lesson will be dedicated to the right to personal data protection within the framework of human rights and the Czech legislation.

The fundamental rights guaranteed both by the Constitution and the Charter of Fundamental Rights and Freedoms include the right to protection of private and family life. It will be explained in this context why personal data must be protected and how such protection is ensured, and what is the relation of the Personal Data Protection Act to the European legal rules (i.e. how and why the Czech legislation is harmonized with European law). In particular, it will be explained that personal data are a key to our privacy, which is one of the basic values of our civilization.

Explanation will also be provided with respect to the principles of personal data protection and the "balance principle", which ensures equilibrium between personal data protection and security (this aspect is important especially in relation to the topical issue of terrorism), as well as a balanced relation between the

general Personal Data Protection Act and the special laws that also provide for personal data protection. In the interest of preserving civil rights, it is increasingly important to be able to enforce the right to privacy and to be aware of the fundamental legal provisions, on the basis of which this right can be exercised.

One lesson will be dedicated to the subject of personal data protection in schools. The Office has experience with personal data protection related to a number of areas where personal data are processed. Personal data are also processed in schools. Explanation of these issues will be based on the principles of personal data protection that must be maintained from the viewpoint of Personal Data Protection Act and from the viewpoint of protection of privacy. On the basis of their practical experience, the teachers will be able to raise questions related to situations which they must face up within their educational activities.
Two lessons will be dedicated to the possibilities of applying protection of personal data and privacy in the framework of specific subjects (for more details cf. section 5).

2. **Form:**

A lecture followed by a discussion with the lecturers concerning specific situations or issues.

3. **Educational goal:**

In relation to approval of the Personal Data Protection Act, No. 101/2000 Coll., and establishment of the Office for Personal Data Protection (hereinafter "the Office") in 2000, the media have been paying increased attention to the aspects of personal data protection as an extremely important part of rights of each individual. Although the general awareness of this aspect is relatively high in the Czech Republic, also thanks to activities of the Office, almost no or very little attention has been paid to certain social groups in this respect. These groups undoubtedly include children and youth. However, in the near future, the current students of elementary and secondary schools will gradually become adults and bear the related political and economic responsibilities. Therefore, their knowledge of personal data protection must be continuously raised so as to ensure that this issue is not out of their interest at a time when they can affect the future of the society as a whole.

Schools are amongst the most important information channels whereby the students of elementary and secondary schools can be acquainted with the subject of personal data protection. However, information provided to the students within the subjects of basic social science, history, information and computer technology must be correct and also linked with specific examples of the practical situations involving protection of privacy and personal data. Therefore, the Office for Personal Data Protection has created an educational program in the framework of DVPP, whose aim is to prepare the teachers at elementary and secondary schools for topics in the area of personal data protection and enable their incorporation in the educational programs of individual schools.

4. **Number of hours + educational goal:**

A lecture consisting of 4 teaching hours

5. **Number of participants and specification of the target group of teachers:**

Four workshops will take place during the school year; a maximum of 40 persons may participate in each workshop.

The primary target group consists of teachers of the following subjects:

subject	Specific educational goal related to the given subject
Czech language and literature	ability to perceive the concept of privacy and personal data protection in various time periods on the basis of a literary text or a work of art
basics of social sciences	personal data protection and protection of privacy in the context of human rights, law and psychology
history	development of opinions on human privacy, its value and establishment of personal data protection in various time periods within the development of the European civilization, influence of totalitarian regimes on the perception of protection of privacy
mathematics, information and computer technology	protection of personal data, their securing in automated processing – security within the Internet, principles of administration of computer technology with respect to data protection, danger of identity theft, modern equipment in personal data protection (tapping, RFID, database systems), principle of electronic signature
biology	possibilities of taking DNA samples, their subsequent processing for verification or identification purposes, different approaches to DNA databases in other countries, creation of databases of fingerprints and other personal identifiers, sensitive data in health care; human privacy – privacy of animals

6. Place:

Office for Personal Data Protection
Pplk. Sochora 27
Prague 7
If teachers from distant regions show substantial interest in this subject, the Office is able to provide a lecture in the given regional capital.

7. Professional guarantor:

RNDr. Igor Němec
President of the Office for Personal Data Protection

8. Material and technical background:

The Office will provide its premises including the necessary audiovisual equipment. Individual participants in the workshop will be provided with information materials.

9. Manner of evaluation of the program:

After the lecture, the participants will have the opportunity to express their opinion on the contents of the lecture and raise additional questions; the participants in the workshops will be presented with a test and a questionnaire; correct answers will be a precondition for granting a certificate on completion of the course.

10. Calculation of anticipated costs (table):

The price per participant equals approximately CZK 300. However, the exact price will always be calculated for each workshop. The aforementioned price is based on the following assumptions:

In case of workshops taking place at the Office for Personal Data Protection, the meeting room and premises will be provided free-of-charge. If the workshop takes place outside the seat of the Office, the costs of renting the premises and equipment will have to be paid.

The prices for DVD, VHS and printed materials that will be provided to the participants in the workshop are included.</P< li>

PRESS CONFERENCIES

The regular press conferences primarily balance the work of the Office in the previous period and provide information on the control activities of the institution, which is its primary statutory duty; however, they also provide an overview of the cases that have been opened in relation to personal data protection with the contribution of the media or specific journalists. However, each of the press conferences also pays attention to a current topic in the area of personal data protection. This is aimed at improving the public awareness of the aspects of personal data protection on the basis of problems that are encountered by the citizens and that affect the quality of their private lives. On 2007, these topics included, in particular, use of camera surveillance systems and raising awareness of personal data protection within the Schengen Information System (SIS) within the context of accession of the Czech Republic to the Schengen area.

The Office continued to fulfill its consultancy tasks towards the media in 2007. The questions raised by the journalists are often concerned with much more complicated issues than in early periods of its existence. The journalists also address the Office with confidence by telephone with questions given to the media by the public and, of course, they also expect information on other sources that could help them find the solutions awaited by their readers.

The regular press conferences have also resulted in a repeated increase in the number of news articles, sometimes very extensive.

Press releases and materials provided at press conferences are available at all times in the relevant section of the Office's website.

PUBLISHING ACTIVITY - DISSEMINATION OF NEW EUROPEAN AND GLOBAL FINDINGS

In 2007, the Office issued four editions of the Journal. The number of editions was the same as in the previous year.

The Information Bulletin of the Office is a quarterly, intended for wider public than the Journal. It consistently aims at raising awareness of personal data protection and provision of information on the most important global events concerning protection of privacy and, simultaneously, describes the foreign contacts and position of the Office.

Within the campaign coordinated by the Ministry of Interior of the Czech Republic in relation to accession of the Czech Republic to the Schengen area, the Office prepared the text of a leaflet concerning protection of personal data within the SIS (Schengen Information System).

OTHER MEANS OF COMMUNICATION

The Office's website was enriched in the relevant year particularly by extending the section dedicated to youth – including an entertaining games.

Extension of the website by the special "Schengen" section naturally accompanied the activities of the Office connected with its new supervisory duty towards the Schengen Information System.

Already in 2006, the Office implemented an extensive information project for the citizens: in cooperation with BENY TV, it prepared 13 parts of the series "Ignorance does not excuse, or Every one has secrets", which was broadcast by the Czech Television at the end of 2006. The series was repeated by the Czech Television in the summer of 2007. There is no doubt that, thanks to this schedule, the information on the Personal Data Protection Act reached a broad public.

The competition for children and youth entitled " My privacy! Don't look, don't poke about!" was announced at the January press conference and was supported over a period of four months by Czech Radio 2 – Prague, the Ministry of Education, Youth and Sports, server Alík.cz, Radio Hey and the International Festival of Films for Children and Youth in Zlín. Previously issued Information Bulletin No. 2/2006 intended for children and their parents was used in the context of this competition.

The works of the children and youth sent to the competition were exhibited at the International Festival of Films for Children and Youth in Zlín (hereinafter MFF Zlín) and the winners of the competition were also awarded at the festival. The winning classes of children were invited to the Office for Personal Data Protection where they met the President of the Office and where a debate was held, emphasizing not only the right to privacy, to which personal data are a key, but also the need for respect for privacy of others, which was symbolically also manifested by invitation of friends of the winners.

A workshop within ongoing education of pedagogic workers also took place during MFF Zlín. The workshop was also organized in December for the Czech Schools Inspectorate.

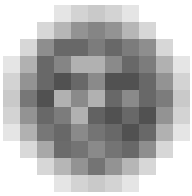
A specialized workshop was provided by the Press Department for seniors who participated in October in the workshop organized by the 3rd Faculty of Medicine of Charles University. It is clear that attention will have to be paid to this generation also in the coming year. The project of cooperation of the Office in activities organized for seniors next year arose within the workshop at the 3rd Faculty of Medicine.

Within its competence and limitations, the Office also cooperates with the Iuridicum Remedium association. The employees of the Press Department were also, as usual, present to the awarding of "anti-prizes" Big Brother, which are awarded by Iuridicum Remedium, and they also participated in presentation of the movie Eye of the Big Brother on use of camera surveillance systems.

LIBRARY AS A PROFESSIONAL BACKGROUND

The professional library of the Office provides professional background for its own employees; however, it also serves permanently for students of secondary schools and universities. In addition to the regularly supplemented books and periodicals (in 2007, the library was extended by 51 books), the library has repeatedly served for students seeking specialized books or periodicals on personal data protection. In this respect, the library provides unique books.

The Office also files all information presented by electronic media with respect to personal data protection.



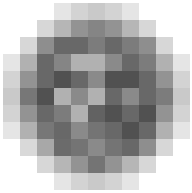
Informatics

The IT Department focused on several main areas in development of the IT system in 2007:

1. Security of the information system
2. Central storage of documents
3. Completion of replacement of personal computers
4. Change in the database platform

Office for Personal Data Protection and its services within e-Government in the Czech Republic

From the viewpoint of sophisticated on-line services, the Office for Personal Data Protection provides 3 basic e-Government services: the website of the Office contains the register of personal data processing together with an on-line form for submission of notifications of data processing; it is also possible to lodge a complaint about unsolicited commercial communications; and information may be obtained at the website pursuant to the Act on Free Access to Information.



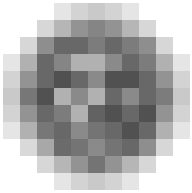
Personnel of the Office

Given the urgent need to complete the preparation for full involvement in the Schengen cooperation and to ensure preconditions for the performance of control and supervisory activities in this area, from both theoretical and strategic viewpoints, as well as from the viewpoint of organization, Resolution of the Government of the Czech Republic No. 633 of June 11, 2007 increased the number of positions at the Office by 5 as of July 1, 2007; thus, in the middle of 2007, the Office had 96 working positions.

As of December 31, 2007, the Office for Personal Data Protection had 92 employees.

Classification of employees of OPDP according to education and sex – as of December 31, 2007

Education	Men	Women	Total	%
Basic	0	0	0	0,0%
Vocational trainingyučen	0	0	0	0,0%
Secondary vocational	1	1	2	2,2%
Full secondary general	3	8	11	12,0%
Full secondary vocational	6	16	22	23,9%
Higher vocational	0	1	1	1,1%
Bachelor's	1	0	1	1,1%
University	36	17	53	57,6%
University + higher qualifications	1	1	2	2,2%
Total	48	44	92	100,0%



Economic Management of the Office

The budget of the Office was approved by Act No. 622/2006 Coll., on the State budget of the Czech Republic for 2007.

Survey of use of the budget in 2007

Budgetary item	Name of indicator	Approved budget for 2007 in thous. CZK	Modified budget for 2007 in thous. CZK	Actual facts pursuant to the accounting records as of Dec 31, 07 in thous. CZK	Fact/modif. budget in %
	TOTAL INCOME	**0**	**0**	**41 052,29**	**0**
501	Salaries	34 718	36 607	37 069,05	101,26
5011	Salaries of employees	26 314	27 635	28 097,05	101,67
5014	Salaries of employees derived from salaries of constitutional officials	8 404	8 972	8 972,00	100,00
502	Other payments for performed work	2 474	2 474	2 333,31	94,31
5021	Other personnel expenditure	2 174	2 169	2 028,31	93,51
5024	Severance Pay	300	305	305,00	100,00
5026	Severance Pay	0,00	0,00	0,00	0,00
503	Mandatory insurance premiums paid by the employer	12 912	13 574	13 732,20	101,17
5031	Mandatory premiums for social security	9 592	10 084	10 203,12	101,18
5032	Mandatory premiums for public health insurance	3 320	3 490	3 529,08	101,12
513	Purchase of materials	5 758	4 920	2 846,83	57,86
514	Interest and other financial expenditure	0	55	10,07	18,31
515	Purchase of water, fuels and energy	1 910	1 925	1 158,04	60,16
516	Purchase of services	18 040	18 927	12 942,74	68,38
5167	Training and education	1 550	2 452	1 787,33	72,89
517	Other purchases	6 251	6 803	4 542,39	66,77
5171	Repairs and maintenance	2 360	2 240	1 003,03	44,78
5173	Travel allowances	2 500	3 134	2 815,51	89,84
518	Advance payments provided	0	0	0	0
519	Expenditures related with non-investment purchases	2 280	2 390	2 182,60	91,32
5342	Transfers to the Social and Cultural Needs Funds	694	732	740,75	101,20

Budgetary item	Name of indicator	Approved budget for 2007 in thous. CZK	Modified budget for 2007 in thous. CZK	Actual facts pursuant to the accounting records as of Dec 31, 07 in thous. CZK	Fact/modif. budget in %
5346	Non-investment transfers to the RF			3 995,44	
536	Other non-investment transfers to public budgets	25	25	8,31	33,24
542	Compensation to citizens	60	60	0	0
5429	Other Compensation to citizens	60	60	0	0
	TOTAL CURRENT EXPENDITURES	85 122	88 492	81 561,73	92,17
611	Acquisition of long-term intangible assets	3 420	3 908	4 146,94	106,11