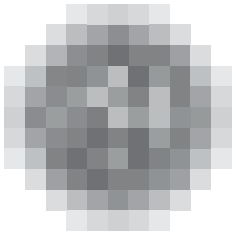
Your personal data can become the gate
to your privacy. It is up to you who you
enter, who you let pass through and wh
you leave standing in front of the gate.



the office
for personal
data protection

ANNUAL REPORT 2006

Year 2006 from the Viewpoint of the President of the Office

Reflecting on the fundamental events that occurred last year and that characterize the work of the Office, I should note particularly our joint efforts to increase the effectiveness of our supervisory activities. To this end, a change was made particularly in the conditions for the work of the inspectors: an adequate staff was provided in the form of working teams; this was reflected in the new organizational structure of the individual inspectorates. The inspectors were provided with greater powers in the area of administrative decision-making on imposing fines for breach of duties in personal data processing. On the other hand, the Office improved the comfort of personal data controllers and provided them with an opportunity to file registration forms electronically.

Foreign activities and relations played an important role in the work of the Office in 2006: this included particularly implementation of substantial part of the European Commission Program "Support to the Commission of Bosnia and Herzegovina", where the Office acted as the main coordinator and professional guarantor with respect to establishment of a new supervisory authority.

In the framework of preparations for accession of the Czech Republic to the Schengen Information System, the Office drew up a thorough survey of its new responsibilities in this area. It was also necessary to create the conditions required, from the viewpoint of personal data protection, inter alia, by the European evaluation mission, whose review yielded favorable results for the Office.

The Office also commenced active preparations for a public awareness campaign coordinated by the Ministry of Interior, which will take place prior to accession of the country to the Schengen area.

The Office concentrated on raising public awareness of personal data protection. Being aware of the force of television broadcasting, we promoted and participated as co-authors in a 13-part series dedicated to personal data protection, which was broadcast by the Czech Television in the period from September to December under the title "Ignorance does not excuse, Every one has secrets". Each of the parts was watched by 160 000 to 310 000 viewers. Within preparations for the Data Protection Day (January 28, 2007), the Office created a strategy of influencing the young generation: it issued a special volume of its Bulletin for children and youth and obtained accreditation from the Ministry of Youth, Education and Sports for its program entitled "Personal Data Protection in Education", which will be implemented in the framework of ongoing education of teachers.

However, in my opinion, the most important activity of the Office includes consistent monitoring of issues in the area of personal data protection within the Czech legislation. Indeed, I do not consider it appropriate that the Czech Republic has only average ranking in foreign evaluation (specifically, by Privacy International) from the viewpoint of the legal preconditions for personal data protection. The unsatisfactory result was caused, inter alia, by excessive use of tapping. I considered it necessary to direct increased attention of the Office at this area, particularly from the viewpoint of securing potential access to the relevant police documents. In my opinion, it is very disturbing that the controlled system of handling of recordings by the police is not in full accord with the funda-

mental principles of legal protection of this information. It was ascertained, inter alia, that an alarmingly high number of persons can access police recordings. Thus, in my opinion, it is currently impossible to effectively prevent leakage of recordings to the media.

Both topical and persisting issues can also be found in a number of other areas of our legislation from the viewpoint of personal data protection:

The Office has been facing long-running pressure from the members of the general public who claim protection of their privacy in relation to easy access to public registers, such as the Land Registry and the Commercial Register. In this relation, the Office has been repeatedly addressed by citizens who complain about abuse of their personal data; however, given the existing legislation that permits inadequately regulated use of the registers, the Office is unable to provide for a satisfactory solution.

The Office has also received repeated complaints from entrepreneurs related to the form of tax identification numbers which correspond to their birth numbers. Unfortunately, this again is based on the law, which was adopted without respect to the objections of the Office; furthermore, although it is a mandatory commentary place within the legislative process, the Office was not even provided with the draft legislation. Thus, we must tolerate the legislation, even though we believe that the form of the tax identification number jeopardizes the citizens' privacy.

Complaints were also lodged with respect to the exchange of personal data of clients between the Czech Television and the Czech Radio which is permitted by the law (i.e. this legislation is also unsatisfactory from the viewpoint of protection of privacy).

The Office is concerned by an amendment related to the national health registers that was approved in 2005 and that will come into effect on January 1, 2007: in relation to the National Register of Users of Medically Indicated Substitution Substances, it is no longer true that data on the patient and on treatment by a substitution substance may be included in the register only with the patient's consent. Unfortunately, personal data are rendered anonymous only after expiry of 20 years from the year of notification of the data. Thus, the principle of protection of sensitive data is seriously neglected.

On the contrary, the Office welcomes the amendment to the Act on Health of the Population which is currently being discussed by the Parliament as parliamentary press No. 83 (January 2007), as it has long strived to ensure that the citizens are enabled access to their medical documentation. It also welcomes the citizens' right to freely decide as to who shall not be allowed access to their medical documentation.

In my opinion, the right to protection of privacy and the right to personal data protection could be fundamentally infringed by the hastily discussed and adopted amendment to the Code of Criminal Procedure and the Act on the Police, related to the conditions for processing genetic data for the purpose of investigating and preventing criminal activities. While no objections can be made with respect to the contention of the drafting party that samples of biological material withdrawn by force could contribute to detection of criminal activities, it is questionable why legal rules were not specified in detail both for the actual acquisition of the biological sample and for its further processing and storage of this information for the needs of the police.

Based on amendment to the Act on Travel Documents, with effect from September 1, 2006, the Office has been the competent authority in the first instance in procedures on misdemeanors and administrative offences consisting in illegal processing of data on data carriers with biometric data. From the viewpoint of personal data protection and particularly with respect to the requirement for purpo-

seful processing of the data following from the new possibilities based on automated processing of personal data and specification of procedures in their use (motivated by the effort to ensure more secure verification of identity), it is necessary that the competent governmental bodies review and, if appropriate, reduce duplicate personal data, identification elements and the contents and form of identity documents also in other activities.

The number of complaints concerned with labor-law relations was much higher in 2006 than in the previous years. These relations are characterized by the prevailing unequal position of an employee with respect to the employer, already during the selection procedure. The Office assumes that the obligations of the future employer towards the job applicants are often breached; however, these instances are more or less concealed.

The Office dealt with (and must still deal with) a case which required that a position be drawn up in relation to protection of personal data in court files. In this relation, the Office issued a position entitled "Supervisory Powers of the Office for Personal Data Protection in Relation to the Performance of Advocacy" (Position 7/2006). This issue requires further negotiations of the Office with the Bar Association.

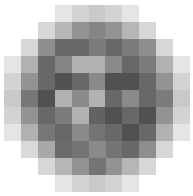
I have listed the main issues encountered by the Office during the previous year and, as I have implied, these issues cannot be resolved merely by applying the general Personal Data Protection Act. In conclusion, I should also mention an extensive topic that, in my opinion, very aggressively endangers privacy and that will have to be dealt with by the Office in the future:

According to our findings, development and operation of video surveillance systems has dramatically increased and has become a social phenomenon. Indeed, the area of operation of video surveillance systems with recording equipment is not regulated by any separate legal regulation and the assessment of its legality can be based only on the general legislation, which includes, in addition to the Personal Data Protection Act, particularly the Civil Code and the Penal Code. The issue of utilization of candid cameras and use of personal data by journalists remains practically unregulated from the viewpoint of protection of privacy and the consequences of its breach. In this relation, the Office will exert increased pressure particularly on those entities that associate journalists or utilize the products of their work so that clearer rules are adopted for ethical conduct of journalists in personal data processing.

Thus, if privacy, as one of the basic values of our civilization, is to be preserved, it is necessary that all legal rules are drawn up with respect to it and that the Personal Data Protection Act is not arbitrarily conceived as a scare or, in other cases, as a harmful legal regulation or insurmountable obstacle where exemptions must always be sought; shortly, this legal rule, which belongs to those that do not impose obligations on citizens, but rather provide for their protection, should not be a target within the fight between various interests seeking for their legal basis.

Igor Němec

Table of Contents



Activities of the Office in Figures – 2006

Enquiries	E-mail inquiries	1564
	Inquiries received by mail	10
Complaints		476
Control activities	Total number of inspections	113[1)]
	completed	77
	according to the plan	14
	ad hoc inspections	99
Unsolicited commercial communications	Total number of instigations	1 503
	Total number of administrative offences	88
	Imposed fines	88[2)]
Administrative punishment	Total instigations received	83
	Decisions on imposing a fine	64
Registration	Total number of notifications	28 591
	Notifications lodged in 2006	1 450
	Total number of cases of processing registered	26 249
	Number of cases of processing registered in 2006	1 195
	Total number of controllers registered	23 073
	Number of controllers registered in 2006	945
	Total number of registrations cancelled	827
	Number of registrations cancelled in 2006	92
	Total number of notifications on a change in the processing	1 597
	Number of notifications on a change in the processing in 2006	178
	Total number of applications for transfer of personal data abroad (Article 27 of Act No. 101/2000 Coll.)	38
	Decisions on authorization of the transfer of personal data abroad	18
	Decisions on rejecting the transfer of personal data abroad	0
	Proceedings discontinued pursuant to Article 30 of Act No. 71/1967 Coll. on request of the party to the proceedings	1
	Other decisions	12

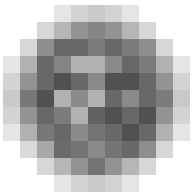
Commented legislative drafts	Acts	55
	Decrees	108
	Regulations of the Government	34
	Other	81
	International regulations	23
Institutions on whose materials (not only of legislative nature) comments were provided	Czech National Bank	7
	Czech Mining Authority	1
	Czech Geodetic and Cadastral Office	1
	Czech Radio	1
	Czech Statistical Office	4
	State Office for Nuclear Safety	1
	Industrial Property Office	1
	Office of the Government	2
	Legislative Council of the Government	14
	Ministry of Informatics	22
	Ministry of Environment	31
	Ministry of Labor and Social Affairs	14
	Ministry of Transport and Communications	19
	Ministry of Interior	34
	Ministry of Foreign Affairs	13
	Ministry of Education, Youth and Sports	16
	Ministry of Justice	20
	Ministry of Health	30
	Ministry of Finance	25
	Ministry for Regional Development	11
	Ministry of Culture	23
	Ministry of Industry and Trade	22
	National Security Office	4
	Administration of the State Material Reserves	1
	Unassigned files	1

Personal consultations	Consultations provided to citizens and institutions	44
Lectures, seminars	(active presentations)	34
Materials published	Journal of the Office (number of editions)	4
	Bulletin of the Office (number of editions)	4
	Positions of the Office / "On Practical Issues"	8 / 1
	Translations of foreign documents	13
	Press releases and communications for the media	15
	Additional basic documents for the media: Agency service, press, radio and television, electronic media	305
Press conferences	Regular press conferences of the Office	4

[1] *113 inspections were commenced in 2006. A total of 77 inspections were completed, of which 12 inspections were commenced in 2005.*

[2] *In 87 cases an order was issued; 1 fine was imposed by a decision*

(The table depicts the state of affairs as of December 31, 2006.)



Supervisory Activities of the Office

I. General

The performance of supervision in the area of personal data protection has constituted the core of activities of the Office since its establishment.

When the Office was established in 2000 as an independent supervisory body of the State, it was primarily intended to monitor and observe the developments with the aim to prevent illegal processing of personal data. As the priority in the coming years lay particularly in the anticipated accession of the Czech Republic to the European Union, the results of the Office's supervisory activities had effects not only in the area of control, but also in the sector of legislation, in the sense that pressure was exerted towards future regulation of legal relations in cases where internal legal rules and conditions for personal data processing in the Czech Republic were not in full harmony with the conditions and principles for personal data protection in EC.

Thus, the Office, which has not yet been given its own legislative initiative, has often found itself in a difficult position where, on the one hand, the public rightly expected expeditious and effective intervention by the Office, particularly with respect to State powers and public administration performed by governmental bodies, and, on the other hand, legal regulations provided and still provide, in spite of the generally applicable principles of privacy protection, for further and more extensive authorizations or exemptions related to personal data processing beyond the scope of the Personal Data Protection Act, both in private law and in public law. Indeed, when the Office's attempts to enforce its opinions and control findings with respect to the special conditions of personal data processing in a certain area are confronted with its actual supervisory competence, the Office must often surrender its categorical viewpoint given the existence of a special regulation that prevails over the Personal Data Protection Act. However, the basic legal conditions are thereby unevenly applied to processing and protection of data and certain groups of controllers are favored solely because their activities are defined by a special regulation, even though no such regulation should in fact exist in the framework of the general principles of protection of privacy and protection of personal data.

Act No. 348/2005 Coll., on radio and television fees and amending some acts, as amended, which came into effect this year, is a good example in this respect; in its framework, new conditions were established for collecting radio and television fees, including the manner of keeping records of payers.

Although, during discussion of the draft law in the Chamber of Deputies, the Office pointed out inadequacies in this regulation, which grossly infringes on protection of the private-law relationship of a citizen to his property, this legal regulation allows for processing of detailed specific information on real estate owned by the payer and his family or persons living with him in a common household for the purposes of collection and payment of fees for receiving radio or television broadcasting.

This is based on the new regulation, i.e. the cited Act on Radio and Television Fees, which stipulates that the supplier of electricity is obliged to notify the broad-

caster, at his request, of customers (natural or legal persons), i.e. potential or existing payers of the fee, with whom the supplier has concluded a contract for supplies of electricity. Within 30 days of delivery of the customer's application, the supplier of electricity shall provide the following data, in addition to the address of the consumption site: the name(s) and surname, date of birth and permanent address (for foreigners, the place of long-term residence) of a natural person, the name, surname or business name, the place of business and identification number of a natural person who is an entrepreneur, the business name or designation, legal form, registered office and identification number of a legal person, the name, seat and identification number of an organizational body of the State or territorial self-governing unit. In addition to this authorization to keep such an extensive database, statutory broadcasters are authorized to provide each other with data from the records of payers of fees for the purposes of ascertaining or verifying their identity.

As it can be expected that both the Czech Television and the Czech Radio will hire a private entity to collect and exact the fees, including search for persons in delay with payment or search for persons avoiding payment, it will also be interesting to monitor the ratio of the broadcaster's costs connected with collection of fees and the amount of fees actually paid. The fact that our society still seems to be surprised by the legal fact that information on our personal property will be available to some other entity, without us being able to prevent this (this information is provided even if the fees are duly paid), leads the Office to the conclusion that the force of private rights that are protected by the constitutional charter of rights and freedoms has been suppressed in favor of another private right – the right to payment for a provided service; thus, the Office finds itself in a position where it must officially respect this legal situation, even though it disagrees with it and, given its role, cannot agree with it.

However, not only the position of the Office itself is in question. Nine citizens addressed the Office for Personal Data Protection in 2006 in relation to the information campaign pursued in 2005 (however, more than 46 persons lodged a complaint in 2005 and 2006) with a request for examination of the state of affairs (complaint) concerned with processing of their personal data or personal data of their family members in relation to collection of fees for radio and television broadcasting. Given the number of complainants, the Office resolved to carry out an inspection concerned with the above-specified matter; however, the Office could only come to the conclusion that the procedure employed by the Czech Television, as the personal data controller, was in accordance with the Personal Data Protection Act and minor shortcomings that were found were remedied by the controlled entity.

Another example where legislation has been adopted in the Czech Republic that fundamentally violates the right to protection of privacy and the right to personal data protection consists in the manner of discussing and approving amendments to the Code of Criminal Procedure and the Act on the Police, related to the conditions for processing genetic data for the purpose of investigating and preventing criminal activities. This year, at the instigation of the Minister of Interior and without proper analysis of the true state of affairs, the Government and then the Parliament discussed and approved an amendment to the law that extends the authorization of the Police to collect and subsequently process biological material, i.e. genetic information, the DNA of individuals. According to the new wording of Article 42e (1) of Act No. 283/1991 Coll., on the Police of the Czech Republic, the following procedure is applicable: a police officer who, in performing the tasks of the police, cannot obtain personal information permitting further identification in any other manner is authorized, with respect to persons accused of an offence, per-

sons serving imprisonment for an intentional offence, persons subject to protective treatment, or persons who have been found after search has been declared and who do not enjoy full legal capacity, not only to take dactyloscopic prints, determine physical characteristics, perform measurement of the body, take visual, sound and similar recordings, but particularly **to take biological samples permitting obtaining of genetic information**.

While the Office fully endorsed the legal regulation of the conditions for withdrawal of genetic material, no one, except the Police, is actually aware of the manner how the obtained information is further processed. Neither the Parliament nor the Government has discussed this matter, although the manner of withdrawal and subsequent provision and processing of this information, its storage and access to the stored information, including liquidation of the originally withdrawn samples, is extremely important from the viewpoint of protection of privacy of those persons who were obliged to suffer the withdrawal, either pursuant to the former regulation or under the new law. Certainly, no fundamental objections can be made with respect to the contention of the drafting party of the amendment to the Code of Criminal Procedure and the Act on Police that samples of biological material withdrawn by force could contribute to detection of criminal activities; however, it is questionable why no legal rules were simultaneously specified, in addition to the actual acquisition of the biological sample, for its further processing, as it is generally known that there is the National DNA Database in the Czech Republic, which is kept by the Criminological Institute, which is part of the Police of the Czech Republic.

In the above-described situations, it is up to the Office to perform all its inspections within its competence in the framework of the boundaries delimited by the Personal Data Protection Act and to review the conditions for personal data processing. For these purposes, the President of the Office set out a new working method in 2006; in its framework, he issues direct instructions for inspection; thereby, the President orders the given inspector to perform a certain control activity in relation to the specific controlled entity in order to ascertain the exact legal conditions for personal data processing at the given controller or processor, as appropriate.

A total of 9 such instructions were issued in 2006, where the inspectors' control activities were concerned with the following entities:

SURVEY OF INSTIGATIONS OF THE PRESIDENT OF THE OFFICE IN 2006

1. T-Mobile, Oskar Vodafone, Eurotel Praha related to processing of clients' personal data.

This complex inspection was carried out simultaneously by three inspectors who came to the following conclusions:

No violation of law was found within the inspection of Oskar Vodafone.

With respect to T-Mobile, the inspection led to modification of the General Terms and Conditions so as to emphasize as much as possible the difference between processing on the basis of law that cannot be influenced by the customers (provided that they have concluded a subscription agreement) and processing to which the operator is not entitled ex lege and, thus, requires the customer's consent. Simultaneously, it is clearly stipulated in which cases the customer may refuse processing of personal data (including revoking of consent) and in what manner this must be done.

As regards Eurotel Praha, the inspection revealed violation of the Personal Data Protection Act and remedial measures were imposed; Eurotel lodged objec-

tions against the inspection protocol; the objections were not accepted and the inspection protocol came into force on May 30, 2006; the Office was forced to discontinue the administrative proceedings in July 2006, as the responsible legal entity ceased to exist.

2. The CorpInvest company in relation to operation of the CERD system – national register of debtors

This inspection, which took place in the period from August to November 2006, revealed that the current activities of the company, however questionable, are not at variance with Act No. 101/2000 Coll.

3. Brož, Sokol, Novák Law Office in relation to publication of personal data connected with activities of the Transport Company of the Capital of Prague

The Transport Company of the Capital of Prague – the inspection did not reveal any violation of the Personal Data Protection Act.

Inspection was commenced in the above-mentioned Law Office and, in spite of the negative attitude of the controlled persons, it was performed and completed with a finding on violation of the Personal Data Protection Act. At the end of September 2006, the Office commenced administrative proceedings which have not yet been validly completed.

4. Criminological Institute in Prague in relation to processing of biometric and genetic data and in relation to the new legal regulation of the relevant conditions

The inspection was commenced on October 3, 2006 and has not yet been completed.

5. Police of the Czech Republic in relation to keeping recordings of tapped conversation within the limits of criminal regulations.

The inspection was commenced on October 5, 2006 and has been completed.

6. Czech Airlines in relation to transfers of personal data of passengers to the U.S. and Canada

The inspection was commenced on December 6, 2006 and has not yet been completed.

7. SWIFT (Society for Worldwide Interbank Financial Telecommunications) and its relations to the banks in the Czech Republic – in relation to transfers of personal data of banks' clients to other countries.

This inspection was connected with the pending inspection of an entity in the bank sector and was commenced on September 12, 2006. In December 2006, it was extended to include control of the state of affairs in other banks.

8. České dráhy, a.s. (Czech Railways), in relation to introduction of the IN customer card.

The inspection was commenced on November 2, 2006.

Another instigation for commencement of an inspection was lodged by the President in late 2006; this instigation was concerned with operation of a video surveillance system and subsequent processing of the obtained personal data of persons present in the vicinity of Radio Free Europe/Radio Liberty in Prague.

The findings obtained in the aforementioned inspections indicate that, using these steps, the Office is able to quickly comprehend the given area and, with agree-

ment of the relevant inspector, impose on the controlled entity (controller or processor) a remedial measure on the basis of the results of the inspection, but also initiate a legislative process or cause the initiation of such process in cases where absence is found of essential legal conditions regulating the relations between the controller and the data subject.

This highly efficient activity is also based on internal reorganization of the section of supervisory activities of the Office which was effected as of January 1, 2006 and gradually implemented during the first half of 2006. A structure of 4 departments of the inspectorate was created for the 7 inspectors, each headed by a chief of inspectorate; thus, control activities are presently performed, together with the 7 inspectors, by almost 20 employees of the Office (5 in each department of the inspectorate). This equals almost one third of all employees of the Office, which provides a sufficient capacity for the control activities of the Office.

The need to create adequate conditions for maintaining particularly young employees within the personnel of the Office is a persisting issue, as the performance of the supervisory activities of the Office, as a state administrative body, is subject to the same remuneration with respect to all employees of the public administration; however, motivation is very important for these employees who work in the field and are often subject to stress situations in dealing with the controlled entities. Therefore, it is necessary to improve the existing relations and conditions in the future and to seek for other opportunities for their utilization. A priority of the Office will undoubtedly continue to be related to the increased need for high-quality supervision in other new areas of social interest. These expectations are connected particularly with inclusion of the Czech Republic in the Schengen Information System and extension of the binding legal framework for relations within the EU 3rd pillar, as well as with processing of biometric data of persons, not only within the new legal regulation of the conditions for issuance of travel documents in the Czech Republic. The high integrity and expertise of the persons undertaking the inspections, as well as their security qualifications and language skills, will be an integral part of the requirements on employees who will be required for new control tasks.

In the framework of their activities, the inspectorates were involved in the entire preparation, performance and legal evaluation of the control activities carried out by the Office's inspectors. Therefore, the inspectors of the Office are provided with full support within their control activities, including subsequent administrative punishment, which forms a new type of activity pursued by the inspectors and also a working task for the employees of the inspectorates, as further specified in the part of this Annual Report concerned with administrative punishment. Inspections performed by the inspectorates were concerned practically with all areas where personal data are processed, both in public and private sectors.

An important procedural regulation of the conditions for proceedings on objections against inspection protocols came into effect on January 1, 2006 in relation to the new legal regulation of the conditions for administrative proceedings, which was introduced by Act No. 500/2004 Coll. As usual, an inspection protocol may be challenged by means of objections within application of supervision pursuant to the Act on State Inspection, No. 552/1991 Coll. The controlled entities use this opportunity relatively seldom; last year, objections were lodged against the inspection protocol in approx. 10 % of cases (a total of 77 inspections were carried out in 2006). An intermediate step, where the inspector made a decision on these objections and which was a mandatory part of this process, was newly abolished. Pursuant to new Article 18 of the Act on State Inspection, a decision on objections may be adopted by the inspector, however, only if he fully accepts the ob-

jections. This procedure was used three times by the Office's inspectors in 2006. When the controlled entity lodges objections against the protocol and the inspector does not fully accept the objections, the case must always be referred to the President of the Office pursuant to Article 18 (1) of the Act on State Inspection.

The President of the Office made decisions on these petitions in 2006 on the basis of proposals presented by a special committee which he established to this end as a special advisory body. Only employees of the Office were members of this committee (employees of the section of supervisory activities and the inspector who has the position of chief inspector during the decision-making process). Thus, while the inspectors in the committee changed, they were, on the other hand, able to participate in decision-making by the Office at a stage in which they specialize, i.e. performance of supervision.

After almost a year of experience with work of this advisory body, the President of the Office accepted the inspectors' requirement that was first expressed in relation to the preparation of amendment to the procedural part of Act No. 101/2000 Coll., where a new concept was presented, according to which the **board of inspectors**, which currently functions "only" as an advisory meeting of inspectors convened by the chief inspector, on whom the inspectors agree for a period of approx. 1 month, would assume another task as a special body of the Office, whose main object of activities would be to unify control procedures and approaches to application of the principles in personal data protection based on the fundamental legal conditions in various areas of the society.

Indeed, the opportunity to discuss objections against colleague's protocol and the possibility of proposing solutions to the President of the Office now provide the inspectors with new findings in the area of control and will improve mutual awareness of the control procedures and, undoubtedly, unify the procedures in the same area of control.

Although the inspectors themselves must be competent to apply supervisory powers in all areas of public interest, over the recent years, the inspectors have specialized to a certain degree, often based on their interest and professional expertise. However, no general comparison of the effects of supervisory competence of the Office on the individual areas of the society has been carried out and the Office is yet to evaluate the effectiveness of supervision.

II. Control Activities of the Office on the Basis of Ad Hoc Inspections

Ad hoc inspections performed by inspectors and their control teams, based on instigations and complaints of individuals, were concerned particularly with the following areas in 2006:

1. Treatment with personal data from the register of population and the register of identity cards.

The Office received an anonymous instigation concerned with questionable treatment with documents produced by the Police of the Czech Republic at its district directorate in Ch. (hereinafter "Police of the CR in Ch."). It followed from the instigation that an unknown person had placed original documents produced by the Police of the CR in Ch., which contained personal data, in waste containers on public premises. Documents that were enclosed with the instigation included extracts from information systems kept by the Police of the CR in Ch. for the purposes of performance of the tasks imposed thereon by law and also printouts from the information system, in which the Ministry of Interior of the Czech Republic keeps per-

sonal data from the register of population and data from the register of identity cards. Although it was most likely that the description of facts in the instigation was incorrect, it was necessary to ascertain whether or not the controlled entity breached its duties following from the Personal Data Protection Act.

The inspection performed on the basis of the aforementioned instigation was concerned with compliance with the duties stipulated by Act No. 101/2000 Coll., on the protection of personal data and on amendment to some acts, as amended, in processing of personal data within the performance of service tasks of the Police of the Czech Republic and, specifically, in requesting and utilizing information from the information system of the register of population and other data files set forth in Article 47 and of Act No. 283/1991 Coll., on the Police of the Czech Republic, as amended, and the records kept by the Police of the Czech Republic pursuant to Article 21 (1) (l) of the same Act.

The inspection performed at the Police of the CR in Ch. revealed that all pages included in the instigation were produced by the Police of the CR in Ch. and were intended for destruction, which took place in January 2006. Some of those documents were printouts from the information system of the register of population and other data files. A majority of the documents were obtained through the program "Inquiries in Information Systems". However, an unknown person took the individual original documents from the bag intended for collection of documents intended for destruction, which was located on the premises of the Police of the CR in Ch., and put them in a container on public premises.

The security failure occurred at the Police of the CR in Ch. particularly because the documents removed from active use were collected and maintained for a short term in the original form, i.e. without substantial destruction using technical means, e.g. a document shredder. Thus, the Police of the CR in Ch. breached its duty stipulated in Article 13 (1) of the Personal Data Protection Act within processing of personal data that were intended for destruction and removed from active use.

The inspection also revealed breach of the duty imposed by Article 14 of the Personal Data Protection Act on the police officers and employees of the Police of the CR in Ch. However, it was not possible to ascertain as to whose breach of duties pursuant to Article 14 of the Personal Data Protection Act caused the misuse of the personal data.

Based on the results of the inspection, the Office commenced administrative proceedings with the controlled entity on imposing a fine for breach of the Personal Data Protection Act.

2. Banking and financial sectors

The Office has traditionally paid attention to this area. The banking sector belongs amongst the major controllers and processors of personal data. The total quantity of processed personal data of the clients of banks and other financial institutions has particularly increased during the last two years in relation to the constantly growing trade in credit products. The efforts to minimize the risks connected with the provision of credit lead to attempts to gather as much information on the clients as possible; however, this information is not always required to secure the credit. Within its control activities, the Office is able to compare the scoring systems employed by the individual banks. It can be very easily concluded that the extent of required information is not always necessary for conclusion of the relevant contract.

As the Czech banking law does not oblige the banks to specify the criteria based on which an application for credit was rejected, the client is unable, not only to express his opinion on the given matter, but also to defend himself in any manner whatsoever. A real problem occurs upon provision of information on an unsuccessful

applicant to the bank register of client information. Thus, an anonymous piece of information derived from the scoring system with a negative output becomes the basis for credit evaluation of the client by another bank that uses a different scoring system. The Office has repeatedly pointed out this practice, which has resulted in the prepared change in the legislative conditions that would enable the client to obtain specific information on the reasons of refusal of a banking service. The Office aims to ensure that the client is provided with specific and open information on the basis of which he would attain a really equal position of an informed client in his dealings with a bank.

Inspections were performed in 2006 in Česká spořitelna, HVB Bank, Živnostenská banka, Raiffeisenbank, Komerční banka and GE Money Bank, and also in the Bank Register of Client Information. The common goal of all inspections was to ascertain the manner of fulfillment of the duty to provide information. It can be stated that while the banks fulfill the duties stipulated by law, they do it in a manner that is not transparent for the clients and, consequently, the clients remain de facto uninformed and, without a legal counsel, they are unable to enforce all their rights following from the law. A typical issue dealt with by the Office lay in the banks' practice used in the provision of information on offered products. Both in Česká spořitelna and in Raiffeisenbank, the inspection ascertained that a client who requested information on a credit product was forced to provide the bank with his personal data and was misled in that he was advised that, otherwise, he could not be provided with information on APR (Annual Percentage Rate – the "price" of credit) and other requisites of the credit. A person interested in this information who had not agreed with the processing of his personal data by the banks, thus found himself in a position where he could not take advantage of his statutory right to information on APR and compare the advantages of the individual offers on the market within the competitive environment. On the contrary, the banks required information that they could process only with respect to their clients. Remedial measures preventing the banks from pursuing this practice were imposed on the basis of the results of the inspections.

Within its control activities, the Office also deals with the aspect of safeguarding personal data of clients in the individual banks. The Office pays great attention particularly to the use of modern technology in communications with the clients. Telephone and internet banking is currently a common practice that has its unquestionable benefits. The other side of the coin consists in the constantly increasing abuse of these technologies, particularly for criminal activities. This includes not only "phishing", which has affected several banks this year, but also the fact that, while the client is obliged to identify himself several times within the use of telephone or internet banking, the banks do not impose this duty on themselves in their terms and conditions. The Office considered it inappropriate that, where the client was reminded by telephone of an outstanding payment, he was forced to identify himself at the beginning of the call without respect to his current location and the possibility that the identification could be overheard by a third person. This is particularly invasive in cases where the birth number is used as an identifier.

3. Unauthorized treatment with personal data

Inspection at a company operating in real estate market

An ad hoc inspection was carried out at request of the Police of the Czech Republic, as there was suspicion that a company had obtained personal data on beneficiaries in restitutions from an abolished territorial workplace of the Land Fund of the Czech Republic in Prague, whom it then approached with an offer to purchase their restitution claims. The Police provided the inspector with part of the materials seized during search. The representative of the company was asked for expla-

nation as to how they obtained the personal data, i.e. the database of clients. No explanation was and could have been adequate, in the light of the evidence collected by the Police of the Czech Republic, and violation of law was proved, namely of Article 5 (2) and Article 11 of the Personal Data Protection Act, with a fine of CZK 10, 000, which was subsequently paid.

Unauthorized treatment with personal data in education sector

A complaint was lodged against the conduct of a school headmaster who sent sensitive personal data to the managers of the schools and members of the board of directors of the founder of the school. The inspection revealed that, after the headmaster proposed that a student leave the school due to his poor results (caused by a certain dysfunction incurred upon birth), the father of the student wrote letters to the managers, members of the board of directors and other persons, where he complained about the approach taken by the headmaster. In an attempt to defend her procedure, she wrote a letter to the same person, in which she, inter alia, noted the state of health of the aforementioned student. This was assessed as violation of the Personal Data Protection Act, namely Articles 9 and 13 of the Act, with a fine of CZK 25, 000.

The procedure of another headmaster, who described in detail the reasons for termination of an employment contract with his employee in a notice of the termination, was considered to be violation of Article 5 (1) (f) of the Personal Data Protection Act. In general, personal data may be processed only in accordance with the purpose for which they were collected.

Personal data processing in offering trade and services

The Personal Data Protection Act is frequently violated in cases where a company processes personal data, while specifying incorrectly or at variance with the Act the purpose, scope and period of processing or where the inspector notes absence of an internal regulation of the controller which is required by Article 13 (2) of the Personal Data Protection Act. In these cases, fines of CZK 10,000 were imposed in summary proceedings on the basis of the control finding.

In case of concurrent violation of other legal regulations, e.g. where copying of personal documents or other conduct of the controlled entity at variance with the Personal Data Protection Act is found, a fine is imposed up to the amount of CZK 25,000.

* One of the controlled companies processed customer's personal data without authorization in spite of his express disagreement with the processing. Given the fact that, on the basis of this instigation, the inspection revealed a systemic error in the performance of duties of a controller, the company was imposed a fine of CZK 15,000.

4. Activities of personal data controller pursuant to special legal regulations

The Office also reviews the activities of a personal data controller or processor in cases where processing is simultaneously regulated by a special act. This included, e.g., activities of an auctioneer and his processing of personal data of a participant in an auction, where the birth number was illegally published in the auction notice.

A special legal framework for processing of personal data of employees where the conditions for processing differ from the Personal Data Protection Act is another example; in this case, the absence of basic information was noted on the basis of Article 11 of the Personal Data Protection Act, including processing of personal data of job seekers based on instigation of the Labor Office.

Summary proceedings were held in these cases, resulting in fines for breach of duties in personal data processing up to an amount of CZK 15,000.

5. Processing of birth numbers

Ad hoc inspections revealed that some major companies manage birth numbers without authorization at variance with the special regulation. Administrative proceedings were held in several cases and fines were imposed in an amount of CZK 30,000, 20,000 and 10,000, respectively.

6. Electronic keeping of accounts

In a letter from the controlled entity, the person submitting the instigation had obtained identification data (the password) which, together with the customer's number, had to be entered upon registration and access to the Phoenix client application (administration of his account). After signing in the Phoenix application operated by the controlled entity, the person submitting the instigation had been forwarded to a website where, rather than his own accounts, the accounts of the XX, a.s. company were displayed. Within that website, the given person obtained information on the individual accounts of XX, a.s.

The inspection revealed that the controlled entity processed personal data of its customers in the SAP and Phoenix information systems in the form of written records.

Although the controlled entity paid great attention to the security of processing of personal data in its internal regulations, it was not able to prevent unauthorized access to personal data contained in the administration of accounts. The inspection also revealed that the controlled entity processed, amongst other things, the birth number and date of birth for identification of authorized customers when it dealt with a request for distribution, supplies or associated services and establishment of a new withdrawal site. The birth number was evaluated as redundant for this purpose.

The controlled entity also breached the duty to obtain the customer's consent to the aforementioned processing in the sense of Article 5 (2) of the Personal Data Protection Act and/or consents of customers – holders of the birth number – in the sense of Article 13c (1) (c) of Act No. 133/2000 Coll., on register of population and birth numbers. Thus, it is clear that a technical means that increases the working and user comfort must be carefully secured and, even in such case, it is necessary that only data required to fulfill the given purpose are processed. Only in such manner will the customers' personal data be duly protected.

III. Control Activities Based on the Plan of Control Activities

The third and traditional area of supervisory activities of the Office is based on the plan of control activities, which was approved for the year 2006, after discussion with the inspectors of the Office, in the following framework and in relation to the experience obtained by the Office in application of its supervisory competence pursuant to the Act No. 101/2000 Coll. and its supervisory competence pursuant to special acts, particularly the Act No. 480/2004 Coll. and the Act No. 127/2005 Coll.

A. GENERAL TOPICS FOR CONTROL ACTIVITIES SPECIFICATION OF THE OFFICE'S INSPECTORS

1. Public administration information systems

Each information system, even if it is operated within the limits of a special act, must respect the general principles of protection of privacy of each natural person, whose personal data are subject to processing, and thus ensure fulfillment of all basic legal conditions in the area of personal data protection.

2. Retail chains

Commercial activities of some business companies in the Czech Republic extensively infringe on the privacy of customers. Communication between the trader and the buyer must respect, not only the conditions for processing of personal data, but also another set of conditions concerning the activities and provision of electronic services by a business company pursuant to the special act. Furthermore, retail chains process personal data of their full-time and part-time employees.

3. Personal data processing with the use of video surveillance systems

For a long time, the Office has been monitoring the increase in the use of monitoring systems in our society. As these measures are not always accompanied by appropriate measures taking account of the potential infringement by these systems on the privacy of individuals, the Office intends to concentrate its inspections on the fulfillment of the controllers‘ duties in processing of personal data in this area.

4. Processing of birth numbers

In relation to the expiry of the transitional period for processing of birth numbers pursuant to the Act No. 53/2004 Coll., increased attention must be paid as to how the controllers comply with the new legal framework of the birth numbers treatment as the basic identifiers of citizens.

5. Supervision in the area of electronic communications

In relation to the increasing scope of electronic communication services and the connected new conditions for processing of personal data, the Office will pay more attention to the new conditions for personal data processing in this area.

B. DESCRIPTION OF THE RESULTS OF INSPECTIONS PERFORMED PURSUANT TO THE PLAN OF CONTROL ACTIVITIES

Some of these activities were performed by the inspectors individually, while others, such as the inspection of retail chains or inspection of tax authorities (more specifically, the system of personal data processing in relation to levying taxes in the Czech Republic), were coordinated in that the inspection was performed by inspectors at several places and at several system levels simultaneously.

1. Inspection of retail chains

In 2006, the inspectors performed inspection of four major supranational retail chains, whose hypermarkets are located in the territory of the Czech Republic. The inspections were concerned with processing of personal data, not only of their customers, but also employees, job applicants and other persons, with whom the company has some other contractual relationship (e.g. suppliers, part-time employees, etc.).

With respect to employees, personal data are processed in accordance with the labor-law regulations. The scope of personal data of employees corresponded to the set purpose of processing, which is required for proper fulfillment of the duties imposed on the employer by special acts. With respect to job applicants, it was ascertained that data are usually required to an extent greater than required for keeping records and selecting job applicants. The controller’s obligation to inform the job applicant of his rights pursuant to the Personal Data Protection Act was not always duly fulfilled.

Shortcomings were also found in processing of personal data of customers – holders of special cards (fidelity cards, etc.). In one case, the inspection revealed breach

of the Article 19 of the Personal Data Protection Act in that the controller, who had ceased to process such data, failed to notify the Office of the manner of these data treatment. However, this breach is not subject to penalty. The Office found no shortcoming in the safeguarding of data from proceedings on claims of defects.

In a majority of hypermarkets, the customers are also monitored by video surveillance systems and recordings are made from these systems. The inspectors thoroughly verified the safeguarding of such recordings in the controlled hypermarkets and they had not ascertained any facts indicating any potential misuse. The recordings are secured, not only against unauthorized access by third persons, but also by employees. However, the acquisition of video recordings is not always in accordance with the law. It was ascertained that persons present on the sale premises (both customers and employees) are recorded in some hypermarkets, which cannot always be considered to be necessary for fulfilling the purpose of protection of property. In some hypermarkets, recordings were even acquired of persons outside the premises of the store. In such cases, the appropriate remedial measures were imposed on the controllers. In general, substantial differences were ascertained in the use of the video surveillance systems. While some retail chains utilize an extensive system of video surveillance, other provide for protection against theft through detectives on the premises of the stores. It is interesting that the losses incurred by a store employing one or two detectives are roughly comparable to the losses suffered by stores with a high number of cameras. Thus, it is questionable whether infringement on the personal rights of the customers by recording their behavior through a video surveillance system is indeed justifiable. The answer must be negative and, in the future, it will be necessary to thoroughly review the need for video surveillance systems in stores, whether by the operators themselves or by the Office within its further control activities.

Activities of the hypermarkets related to detention of persons suspected of theft of goods were also reviewed. These activities are usually ensured for the hypermarkets by hired agencies. It was ascertained that, in cases where such agencies establish personal data of the detained persons, these data are always provided to the police bodies and the hypermarkets do not have access to them.

Repeated breach of the Act No. 328/1999 Coll., on identity cards, was ascertained in a hypermarket chain, where identity cards were illegally copied and the copies collected without the consent of the holders, both the employees and visitors. This retail chain was also guilty of misconduct in that it left freely accessible thousands of survey questionnaires containing personal data of the customers who filled them out during marketing events. Other misconduct consisted in collection of personal data of detained persons suspected of theft without any legal grounds, also in cases where innocence of the detained person was later proved. In addition to other breaches, this retail chain was found to violate the law by operation of the video surveillance system with recording equipment, including inappropriate period of storage of such recordings and, particularly, monitoring of persons and premises that had nothing in common with the activities of the retail chain. The video surveillance system could monitor extensive areas in the vicinity of the store, including roads and houses.

A fine of CZK 500,000 was imposed on the hypermarket chain for the aforementioned infringements.

2. Video surveillance systems

Utilization of monitoring technology, particularly video surveillance systems, has increased dramatically during the recent years. The reason clearly lies in affordability of those systems and the user comfort. Monitoring and recording the behavior of persons, together with storage of these recordings, can be encountered

in the streets, stores, manufacturing enterprises, apartment houses, elementary schools and kindergartens, hospitals, social care institutes, restaurants and churches. However, the justification of acquisition of video recordings in such cases is clearly doubtful.

Therefore, in 2006, the Office also concentrated on the subject of compliance with the controllers' duties in personal data processing in this area. 10 inspections were commenced and 7 of them have already been completed. Inspections were concerned with apartment houses, department stores, a provider of telecommunication services, a printing house of national importance and a school.

The same purpose of recordings acquisition was stated by all the controlled entities, namely protection of property and, as the case may be, persons, without consent of the monitored persons. However, such protection cannot be relied on in cases where the mandatory preconditions for acquiring a video recording (and, thus, also personal data) stipulated by law are not fulfilled. The first and fundamental precondition for acquiring a recording without the consent of the affected person consists in the fact that the acquisition of such recording is necessary for the protection of the operator's (controller's) rights. Thus, all other possibilities of protecting persons and property must first be employed. Simultaneously, it is necessary that the second precondition be met, i.e. no infringement on the private and personal life of natural persons. Indeed, privacy of an individual does not include only privacy of his "four walls"; every individual has the right to a certain degree of privacy also at the workplace, in schools, in stores, in restaurants and in the streets, i.e. in places that are more or less publicly accessible.

It was ascertained that the acquisition of visual recordings was not necessary for vast majority of the controlled entities. On the contrary, the video surveillance system was usually operated only as a precautionary measure, without any previous attempts to secure the property in any other manner. The recordings were used to check the compliance with the working hours (provider of telecommunication services, printing house); the headmaster of the controlled school ascertained whether or not the teachers use the school premises for their private activities. In the apartment house, the video surveillance system "detected" the entity responsible for polluting the entrance door (dog). It is very unfortunate that video surveillance systems are acquired even for such, sometimes absolutely negligible, reasons, even though these systems are capable of substantially infringing on the privacy of individuals. When discussing the inspection protocols with the operators (controllers), the inspectors mostly encountered absolute lack of understanding for the need to protect privacy, human dignity, private and personal life, i.e. values that are declared by the Charter of Fundamental Rights and Freedoms and that are also incorporated in the Personal Data Protection Act.

Furthermore, the operators of the video surveillance systems were also controlled with respect to other duties stipulated by law. The period of storage of the recordings was usually found inappropriate to the set purpose; some entities kept such recordings for several months. The information duties pursuant to the Article 11 of the Act are fulfilled to a very limited extent, usually by means of an informative sign like "the premises are secured by a camera". The security of access to the video recordings can be considered to be a positive aspect, as vast majority of the controlled entities appropriately secured the recordings against any misuse.

All controlled entities that were found to violate the law were imposed remedial measures, including, in some cases, prohibition of operating a video surveillance system and acquiring recordings. **Penal administrative proceedings will be pursued as of 2007.**

3. Publication and safeguarding of personal data by the Police of the Czech Republic with respect to personal data processing within pending criminal proceedings

One of the main topics of 2006 in the Czech Republic that are related to personal data protection and the Office's competence consisted in tapping and recording of telephone calls by the police. This topic was discussed both in the media and by the politicians and it also interested the citizens. A popular aspect of this issue lay in the recording of tapped conversations of publicly known persons, including active politicians. Furthermore, the media published personal data from pending criminal proceedings in investigative reports and, operatively, also in relation to certain cases. The media presentation and discussion in the Chamber of Deputies of the Parliament of the Czech Republic led the President of the Office to order an inspection of the Police of the Czech Republic. Furthermore, on September 7, 2006, the Office received two instigations from a single citizen of the Czech Republic, who complained about publication of the contents of the tapped conversations and other information on criminal proceedings, together with personal data, by the public-service television.

The Police of the Czech Republic, as an entity fulfilling tasks pursuant to the Code of Criminal Procedure and the Act on the Police of the Czech Republic and other applicable regulations, particularly the Act No. 412/2005 Coll., on protection of confidential information and on security qualification, process personal data within the pending criminal proceeding. A report submitted to the parliamentary control body concerned with the use of tapping and surveillance in the sense of the Article 53(a) of the Act on Police of the Czech Republic is a periodical document concerning processing of personal data. A full survey of subscriber addresses (numbers) that were tapped by the Police of the Czech Republic during the relevant period is enclosed with the report. It was found that this was a set of inadequately anonymous data that constituted personal data; this was not prejudiced by the fact that the entity to which a certain tapped subscriber address was formally related could be a legal person.

The Police of the Czech Republic are responsible for personal data processing within pending criminal proceeding only up to the point when they are submitted to some other entity. Responsibility for further treatment with personal data is born appropriately by their recipients, i.e. persons authorized pursuant to the Code of Criminal Procedure, other prosecuting bodies, individual journalists and legal persons who publish or otherwise disseminate the personal data from the pending criminal proceeding.

In relation to the performance of the duty of the Police of the Czech Republic to adopt measures pursuant to the Article 13 (1) of the Personal Data Protection Act (hereinafter "security measures"), it was ascertained as to whether and how the Police of the Czech Republic had defined the responsibilities for personal data processing in the framework of the pending criminal proceeding, how the responsibilities stipulated by the Police of the Czech Republic and the law were enforced and what other organizational and technical security measures had been taken to ensure personal data protection. In the assessment of security measures, the controlled entity based its considerations on the findings of previous inspections performed at the Police of the Czech Republic. It was ascertained and confirmed at individual workplaces and premises of the controlled entity that the security level had not been reduced. **More detailed review was concerned with technical and security measures actively adopted in relation to several specific data files containing information on pending criminal proceeding and in relation to tapping. Several issues were noted within this framework:**

1. From the beginning, a great many persons had access to personal data describing the pending criminal proceeding, both at the Police of the Czech Republic and at other entities: e.g. 4 305 valid user authorizations were recorded for one file, for another file this number equaled 33 300 only in the Police of the Czech Republic. On the basis of the Articles 41 to 43, 55, 55(a) and, particularly, the Articles 59 and 65 of the Code of Criminal Procedure, the persons set forth in those articles are provided with certain documents containing personal data in the form of a counterpart, while other documents are provided in the form of non-individualized copies.

   Information on pending criminal proceeding processed in certain electronic data files of the Police of the Czech Republic are further made available to other controllers for their individual browsing based on a continuous remote access, based on a written requirement or telephone inquiry: three ministries, intelligence services and the National Security Authority.

2. Security measures adopted and utilized by the Police of the Czech Republic are not followed up by any corresponding security measures on the part of the recipients of personal data on pending criminal proceeding. The media in principle publish the obtained personal data, while the procedure of the Ministry of the Interior and the Chamber of Deputies of the Parliament of the Czech Republic in relation to the reports on tapping must be assessed in the light of the principle enshrined in the Article 6 (1) of the Act No. 412/2005 Coll., on protection of confidential information and on security qualification, according to which a natural person may be enabled access to confidential information classified as "Reserved" only if that person requires it for the performance of its office, employment or other activity.

   The variance between the conditions of access to personal data on tapping and recordings of calls at the controlled entity and at the recipients of the periodical report is clear; however, the level of security measures employed by the recipients of the report was not subject to inspection.

3. The security measures that the Police of the Czech Republic are to adopt and implement pursuant to the Personal Data Protection Act are generally compromised by the fact that protected personal data may be published pursuant to other acts. The Article 42(l) of the Act on the Police of the Czech Republic strictly limits the scope of publication to the required data and, simultaneously, stipulates that it must be related to criminal proceeding. The Article 8(a) of the Code of Criminal Procedure authorizes the Police of the Czech Republic to publish personal data directly related to criminal activities. Information on pending criminal proceeding provided in response to an inquiry made by a journalist does not fall within the regime stipulated by the Article 42(k) of the Act on the Police of the Czech Republic. Information provided upon own initiative of the Police of the Czech Republic pursuant to the Article 8(a) of the Code of Criminal Procedure again falls to a different regime.

4. The security risks are related to the telecommunication infrastructure, within which the personal data on pending criminal proceeding are processed. The Police of the Czech Republic are fully responsible only for those measures that may be adopted at the level of applications; responsibility for other measures is born jointly with the Ministry of Interior.

   The performed inspection revealed that the Police of the Czech Republic had adopted and implemented measures to fulfill the duties stipulated in the Article 13(1) of the Personal Data Protection Act and that the adopted and implemented measures are processed and documented. No breach of the set regimes and physical security measures was found on the premises of the Police of the Czech Repub-

lic; there was also no indication of failure to respect the responsibility stipulated by the applicable regulations or internal management acts.

The findings indicate that personal data protection within pending criminal proceeding pursuant to the Protection of Classified Information Act is not too effective as a security measure pursuant to the Personal Data Protection Act; it is more beneficial with respect to the fulfillment of the duty to document the adopted and implemented measures.

IV. Control Activities in the Area of Supervision Pursuant to the Act No. 480/2004 Coll.

The separate section entrusted with handling the subject of unsolicited commercial communications was stabilized in 2006. This issue, including acceptance of electronically lodged complaints with the use of the web form, was entrusted to Inspectorate IV. The rather unsystematic state from the previous years, when several sections dealt with this subject matter, was remedied to a substantial degree. The increase in personnel of the Inspectorate enabled to modify the control processes in order to increase their efficiency. Thanks to a certain specialization within the separate section, it was possible to relatively substantially optimize the control process which otherwise would be entirely unmanageable due to the high number of complaints and the relatively obsolete legal regulation. Indeed, the absence of discretion of the control body, as regards evaluation of the degree of gravity of the allegedly illegal conduct, has been a prevailing setback of the legal regulation. Thus, every conduct must be considered to have the same gravity, even though the individual cases substantially differ, either in the manner of conduct, scope or fault of a certain person.

Furthermore, given the inadequate number of control personnel in relation to the number of complaints, it was necessary to significantly modify the traditional procedure of inspection in situ. A methodology was drawn up to this end, according to which a majority of the required information is obtained through questionnaires, with subsequent analysis of the content of the reports, instead of inspections in situ. This procedure had to be introduced also for the reason of the special nature of business activities on the Internet, as a number of entrepreneurs in this field do not have special business premises and, thus, operate their business at home and often in their free time. Thus, usual official contact with such persons is rather difficult.

Difficulties are still caused by inadequate competence in obtaining operational and location data from providers of electronic communication services, which would facilitate the conviction of offenders of administrative offences in some cases. The cooperation between the Office and these operators could certainly be much improved with respect to implementation of certain measures against entities that utilize the offers of unpaid services (freemails) for the purposes of disseminating unsolicited commercial communications. The Office recorded several such instances and notified the operators thereof in 2006; unfortunately, without any adequate response. On the other hand, there was a considerable response to a campaign whereby the Office approached persons who lodge complaints against unsolicited commercial communications through the Office's web form. The objective was to ensure that these complaints are conceived as the last means to remedy a defective state of affairs where it usually cannot be anticipated that such conduct of senders of the commercial communications was caused by a mistake or technical error. Unfortunately, in a number of cases the opposite is the truth and lodging a complaint

is the first step taken by the affected person. Indeed, in a considerable number of investigated cases there has been no intention to disseminate any commercial communication. Investigation of cases where one or two complaints have been lodged thus prevails and requires a considerable amount of efforts and means.

The persons performing inspection must proceed pursuant to the Act No. 552/1991 Coll., on State Inspection, and cannot apply the Act No. 101/2000 Coll., on personal data protection, which would enable them to impose remedial measures and otherwise improve the control procedure. The fact that the persons undertaking inspection cannot access information on the holders of the IP addresses prevents the detection of persons who conceal their identity, i.e. those who belong to the more serious category. The current options can only be employed in relation to "honest" entrepreneurs, i.e. those who do not conceal their identity, duly operate their business and usually have sent one of their messages to a person who they considered to be their client or to an address which they believed could be used to this end.

In 2006, the Office received a total of 1503 complaints related to dissemination of unsolicited commercial communications. Compared to 2005 (approx. 1000 complaints), this corresponds to an increase by 50 %. A total of 1108 complaints were dealt with. Of the total number of complaints lodged, 255 were found unjustified (particularly because a commercial communication was not involved) and in 76 cases it was not possible to ascertain the sender of the commercial communication. Remedy was ensured in 121 cases without the need to perform inspection. During 2006, Inspectorate IV commenced 163 inspections (656 petitions were dealt with) concerned with compliance with the Act No. 480/2004 Coll., on certain services of the information society and on amendment to some acts (hereinafter "the Act"). Inspectorate IV completed 29 inspections commenced in 2005 and 124 inspections commenced in 2006. Administrative proceedings were commenced in 87 cases and fines were imposed in a total amount of CZK 316,000.

The most common misconduct committed by the senders of commercial communications in the previous years does not differ from the previous years and could be summarized as follows:

1. Many of the controlled entities referred to consent granted over the telephone and almost no one consistently respected the opt-in principle. In this case, it holds that, unless the recipient expresses his consent, disagreement is automatically assumed.
2. Almost no one designated the message as a commercial communication. The messages had all sorts of designations (newsletter, info, new products, etc.). However, the Act on Certain Services of the Information Society stipulates that a commercial communication must be "clearly and plainly" designated as such. Specification that a "commercial communication" is involved must be placed in the identification field of the message so that, where the IMAP protocol is used, the recipients need not download these messages from the server but rather they are able to delete them directly on the server after reading the heading. The same applies to the settings of anti-spam filters.
3. Some providers of internet services contribute to obfuscate the interpretation of the legislation in that they do not send out the commercial communications themselves, but insert advertising footnotes at the end of the messages that they transmit (i.e. short advertising messages placed as a footnote to e-mail). They then claim that these are not separate messages. The thus-disseminated message not only contains all the aspects of a commercial communication and does not allow, e.g., for effective refusal of these messages, but the service provider assumes responsibility for the contents of the entire message, as he has modified the message (the Article 3 of the Act No. 480/2004 Coll.).

4. Some senders use the "blind carbon copy" to send their messages. While they do not communicate to the recipient the addresses of all persons to whom they had sent the e-mail, the recipient nevertheless receives the commercial communication without specification of his own address. This is especially unfavorable if the recipient has several addresses and downloads electronic mail from several servers. Indeed, if he intends to prevent the receipt of any further messages, he cannot do so in a simple manner, as he is not aware to each of his addresses the message was sent.
5. For some providers of electronic services, demonstration of consent is limited to checking off a box in the registration form in the relevant section of the web application. They neglect the fact that such a form can be filled in by anyone (and thus for anyone) if it is not protected by an access name and password. Thus, prior to the actual sending of commercial communications, it is necessary to verify the manifestation of will of "registered" users, e.g. by sending an informative e-mail message on registration, together with the possibility of refusing commercial communications or, preferably, with a request for confirmation or registration details.
6. If commercial communications are to completely comply with the provisions of the law, they must be properly accompanied by a valid address, to which the addressee could directly and effectively send information stating that (s)he does not want the sender to continue sending commercial information. However, if the sender has his database of clients organized according to e-mails, a discrepancy occurs if the delivery address of the client is different from the registered address. Flawless communication requires that the database be supplemented by a different identification element (client number, etc.) and that this element be enclosed with the disseminated commercial communication. Thus, it is necessary to send reports in another manner other than collectively through traditional mail clients.

Development of the legislation

The Act No. 480/2004 Coll., on certain services of the information society, was modified to a certain degree in mid-2006. Amendment to the Act, No. 214/2006 Coll., came into force on August 1; this amendment, also based on evaluation of the former regulation by the European Commission, partially introduced the general principles of opt-out, as it newly enabled to send commercial communications to the customers of the sender (i.e. persons with a previous commercial relation to the sender), as regards an offer of similar products or services, also without the prior consent, provided that the customer has not rejected the use of the details of the electronic contact for sending such commercial communications. Another precondition consists in the obligation to cease sending such commercial communications once the customer expresses his disagreement. The customer must be able to express such disagreement in a simple manner, free-of-charge or at the expense of the sender.

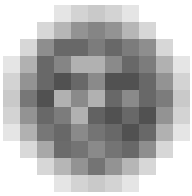
Introduction of the opt-out principle to the subject of sending commercial communications amongst entrepreneurs and their customers admittedly simplified commercial communication amongst these entities. On the other hand, it must be admitted, in the light of practical experience, that this is basically a cosmetic modification of the legislation, as a majority of issues related to unsolicited commercial communications lie in a different sphere. Indeed, commercial communications continue to be used for acquiring new customers, rather than to approach the current ones. In these cases, it is very difficult to obtain the prior consent to sending commercial communications, as the "guaranteed" channel – electronic mail – cannot be used in this case. This is also the reason why this duty is often evaded and constitutes the most common reason for commencing administrative proceedings.

Difficulties still follow from unclear interpretation of the actual definition of a commercial communication, particularly the part of the definition explaining what a commercial communication is not. In contrast, commercial communications do not in-

clude data enabling direct access to information on activities of a natural or legal person or an enterprise, particularly the domain name or e-mail address. Some entrepreneurs, in an attempt to avoid the strict provisions of the law, create electronic messages containing only a link to a website, where the commercial communication consists of the text constituting the contents of the link.

A mention should be made in this respect of "viral marketing" which consists in voluntary dissemination of messages with commercial contents. The voluntariness is characterized as a "friendship service" as the usual interpersonal contacts amongst family friends and colleagues from work are used as communication channels in this case. Furthermore, the commercial communication is not contained in the actual message, which includes only a link to a website encompassing, e.g. an advertisement for goods or services. It is the unambiguous interpretation of the definition, from which it can be derived in a certain sense that a mere link to a website is not a commercial communication pursuant to the Act on Certain Services of the Information Society that causes substantial complications in practice. A future amendment to the Act should certainly provide for more specific definition of this exemption.

However, there has also been a positive shift in public understanding of the need for regulation of privacy in electronic communications. Therefore, the websites of online stores and other companies include ever more often various types of registration forms that transparently provide electronic contact details and, particularly, it enables to provide or revoke consent to sending of commercial communications. Nevertheless, the public opinion on this issue is still not consistent and particularly small and new entrepreneurs conceive the Act on Certain Services of the Information Society as a useless bureaucratic impediment to their business. This concept is usually supported by the fact that a majority of unsolicited communications flow to mailboxes from foreign servers without any regulation whatsoever, which is a problem that understandably cannot be resolved by the Czech legislation. In such inflow of spams, several domestic unsolicited commercial communications appear absolutely harmless and are subject to discussions on the need of their regulation. However, that is absolutely correct as, in addition to the aforementioned aspect of protection of privacy, this phenomenon has its economic aspect as, in a certain sense, it also prejudices proper economic competition.



Complaints handling and provision of consultations

The Department of Complaints and Consultations was established within the reorganization of the Office as of January 1, 2006, with the aim to improve services for the public. Its activities include:

- responses to telephone inquiries
- provision of personal consultations
- responses to electronic petitions
- legal assessment of instigations and complaints

One-year experience showed that combination of the aforementioned tasks within a single workplace – without any increase in the specified number of personnel – was justified and, within the overall context of efforts to improve the Office's control activities – fulfilled the purpose declared in 2005. All cases are dealt with consistently from the beginning, when the citizens approach the Office by telephone, in person or by e-mail with inquiries like "is it correct when … or is this breach of the law?", usually by a single employee of the department, which contributed to the timeliness and quality of further measures. While, in early 2006, the Department of Complaints and Consultations had problems with complying with the thirty-day statutory deadline for resolving a petition, by the end of the same year, this period was reduced to approx. one half. Cases where the petitioners receive responses within several days are increasingly frequent. The subsequent positive reactions document that the Office has taken the right approach in this respect. Thoroughly performed initial legal qualification of the matter, as well as supplementation and verification of the provided facts indicating justified suspicion of violation of laws regulating the area of personal data protection, positively influenced the further procedure in the matter, i.e. performance of supervisory activities of the Office in the form of inspection or proceedings on imposing a penalty for a misdemeanor or some other administrative offences pursuant to the Personal Data Protection Act.

Personal data processing through video surveillance systems was undoubtedly a phenomenon that affected all statistical data in 2006.

Position of the Office No. 1/2006, "Operating Video Recording Systems in the Light of Data Protection Law" of January 2006 was subsequently published in the media and the responses of entities of all categories, including police bodies, courts, public administration, municipal government, economic entities, trade unions, apartment cooperatives and natural persons who are employees, students, tenants of apartments, clients of financial institutions, visitors of retail chains, etc., indicated that this was a very topical subject. The common denominator of evaluation of these very diverse petitions was the statement that personal data processing through a video surveillance system can infringe on privacy of individuals to previously unknown extent and dimensions. This is a dynamically developing area where, along with the new technology and reduction of acquisition costs of the technical means, there is a constant increase in the number of entities utilizing video surveillance systems, even in cases where this has no justification from the viewpoint of the Per-

sonal Data Protection Act, including privacy of tenants in apartment buildings, monitoring of employees at the workplace, monitoring of the conduct of students and pupils in classes, recording public premises within protection of one's own or entrusted property, etc. Therefore, the Office paid increased attention to this issue during the entire year 2006 and, inter alia, by its interpretation, it substantially limited exemptions from the notification duty, practically only to those cases where the use of a video surveillance system is directly contemplated by one of the special generally binding regulations. The second wave of public interest in video surveillance systems came in November 2006, in relation to the decisive and successful protest by students of the Josef Škvorecký grammar school against installation of cameras directly in the classes.

The effect of the number of inquiries, requests, consultations, instigations and complaints related to the video surveillance systems on the overall statistics can be documented as follows: the monthly average of all types of petitions lodged with the Department of Complaints and Consultations in 2006 equaled 153. 178 petitions were lodged in February, 191 in March and 211 in November. Qualified estimates indicate that of the overall number of 8 000 telephone consultations approx. ? concerned the video surveillance systems in some manner.

In addition to the above-described cases, the general public also responded by numerous instigations and complaints to other social phenomena; from the Office's viewpoint, the most important were, e.g., as follows:

- exchange of personal data of clients between the Czech Television and the Czech Radio
- introduction of chip In-cards by data controller Czech Railways (the inspection has not yet been completed)
- utilization of birth numbers in publicly accessible databases (the Commercial Register, Register of Economic Entities, Land Registry)

In relation to adoption of the new legal regulation of the Act No. 348/2005 Coll., whose Article 8 (11) enables statutory broadcasters to mutually exchange data from the records of fee payers for the purpose of their identification or verification, the Office has stated that these legal conditions are not in conformity with the general principles of personal data protection. The importance of this issue is increased by the fact that the databases of viewers of the Czech Television and listeners of the Czech Radio include millions of clients. Several dozens petitions were dealt with in relation to implementation of the Act and the questionnaire survey of the Czech Radio, which required further personal data from persons who owe fees, e.g. telephone number and account number, while not complying with its statutory duties of a controller. It is not excluded that the Personal Data Protection Act was also breached in this relation by suppliers of electricity and the Czech Post (investigation of these cases has not yet been completed).

Unfortunately, it is still common that birth number is considered to be the only unique identifier of a specific natural person which leads to treating thereof at variance with the Act No. 133/2000 Coll., on register of population and birth numbers and on amendment to some acts, as amended. This opinion is also refuted by the new Code of Administrative Procedure; cases of unauthorized treatment with birth numbers are usually directly punished, without the need to commence inspection. This often involves rather tragicomic stories documenting elementary ignorance and low level of legal awareness, where the controller required the birth number from a participant in a ten-hour user course for PC or upon registration in a library and, on the contrary, the clients of a bank were absolutely illogically provided with a list of bank's authorized employees together with their birth numbers.

On the contrary, in its press release for CTK (Czech News Agency), the Office was forced to deny the verbatim wording of the article published in the Právo daily newspaper of December 20, 2006 "Companies forced to modify millions of employment contracts with respect to birth numbers". The contents of the article were misleading and caused numerous inquiries and angry responses of employers. The Office explained that a birth number may be used, inter alia, with the consent of the person, to whom it was assigned. The signature on an employment contract containing the birth number by the employee is a sufficient manifestation of his/her consent and, therefore, in employment contracts concluded by December 31, 2005, i.e. by the end of the transitory period stipulated by the amendment to the Act No. 133/2000 Coll., birth numbers need not be rendered illegible. Employment contracts concluded this year should no longer contain the birth numbers, as for the given purpose (conclusion of a contract), this is a redundant personal data, provided that the contract also specifies the date of birth. This is true notwithstanding the fact that the employer must use the birth numbers of his employees, e.g. for the purposes of health and social insurance or calculation of salary or wage. The Article 13c (1b) of the Act No. 133/2000 Coll. may apply to the use of birth number if this is stipulated by a special act. In that case, the consent of the person to whom the birth number was assigned is not required.

Business persons ask ever more often, why they, i.e. statutory representatives of business companies or individuals operating a business pursuant to special regulations, are not subject to the same personal data protection as other members of the society. The Office is forced to respond in that the Act No. 513/1991 Coll., the Commercial Code, as amended, contains a special regulation of processing of data, including birth identification numbers, registered in the Commercial Register, which is a public list kept in electronic form and which may be perused by any person, who may also make copies and excerpts. Almost identical legal consequences follow from the Act No. 455/1991 Coll., on business in trade, as amended, and the Act No. 337/1992 Coll., on administration of taxes and fees, as amended. The Office must respect this state of affairs; however, it considers that the legislation is inappropriate, primarily because it concerns millions of business persons and statutory representatives. However a change may be brought only by amendment to the aforementioned acts and, as the Office does not have legislative initiative, enforcement of the personal data protection principles is difficult. From amongst dozens of inquiries, instigations and complaints a quote can be made of a letter sent by a physician:

"Dear sir, Thank you for your response. However, as an executive of a limited company, I feel highly discriminated by the law you mentioned (i.e. the Act No. 513/1991 Coll.), as I believe that I am entitled to the same personal data protection as any citizen of this country. I hope that the law will be changed in the future and that the Office for Personal Data Protection will serve every one of us, rather than only some people."

The same state of affairs, including the increasing number of dissenting petitions, exists in relation to another public list – the Land Registry. The obligation of the person who has obtained personal data, including the birth number, from the Land Registry, to use the data only in the manner stipulated by law, is not an adequate remedy for the affected persons, as this is not only the issue of personal data, but also a more extensive infringement of privacy. In the opinion of the Office, the possibility of ascertaining the assets of citizens, i.e. the ownership of real estate, should be unambiguously conditional upon demonstrating unquestionable legal interest.

As regards the categorization of complaints from the viewpoint of typology of breaches of the Personal Data Protection Act, no substantial change was recorded in 2006. The individual breaches thus continue to include unclear specification of the purpose of processing, collection of personal data to a greater extent and for a longer period of time than required for attaining the set purpose, processing of personal data for a purpose other than declared, defects in the consent, which is then no longer manifestation of free will of the data subjects, i.e. voluntary and informed, enforcing the consent under the threat of, e.g., non-provision of the requested service or refusal to sell goods, non-compliance with the information duty, transfer of personal data to third parties or publication of the data without consent.

Some obliged persons continue to address citizens with offers of goods or services on the basis of unclear sources of information on their personal data. Cases were also recorded where the commercial entities sold one another such databases of potential clients. Furthermore, it is relatively frequent that controllers declare the use of obtained personal data for protection of their very unclearly specified rights and legal interests. Another unfavorable phenomenon resulting in breach of the duty to ensure security of personal data consists in repeated presence of documents containing personal data outside the premises where they are processed, including publicly accessible areas. Written materials containing sensitive data, which are subject to stricter protection under the Personal Data Protection Act, particularly from medical records, have also been repeatedly lost. Under the legislation of this country, publication of the names of debtors and non-payers is considered to be inappropriate pressure aimed at enforcing a claim that could cause the affected entity harm in other areas of private and public life; therefore, it is illegal. A brief petition lodged by the mayor of a municipality is an example of this issue:

"I enclose forms which I found on November 18, 2006 in the municipal waste container. They weight approximately 100 kg and concern the entire Western-Bohemian region." Subsequently, it was ascertained that the form of one of the construction-savings companies contained all contact details of a client, personal data of an insurance advisor and data on the concluded contract, including the set target amount, state of the account, client's credibility, etc.

Another issue is related to copying of various types of documents and materials, whereby a number of controllers simplify their work. Copying the identification cards and passports without the consent of the holder is prohibited by special acts, except for cases where this is permitted by some other generally binding legal regulation or international agreement. The Office usually evaluates these cases, which are primarily a misdemeanor that is to be discussed by the competent municipal authority of a municipality with extended competence, also as violation of the Personal Data Protection Act, because they involve collection of personal data redundant for the given purpose (e.g. signature of the holder of the identification card, personal data of his/her spouse).

A specific area, where the number of complaints was much higher in 2006 than in the previous years, consisted in labor-law relations. These relations are characterized by the unequal position of an employee with respect to the employer, already during the selection procedure. Fear of loss of employment is manifested in the highest percentage of anonymous complaints and the Office also assumes that there is a high latency of breaches of the controllers' obligations.

In this relation, it is necessary to make a brief note on the Office's approach to the complainant's identity. There are two basic approaches both in theory and in practice. The prevailing opinion is that every one should bear the consequences

of his conduct. However, it is also argued that the complainant merely enforces his right to the protection of privacy stipulated by law and, therefore, as a rule, he should not be liable to any sanctions potentially imposed by the controller. The Office believes that the complainant's right to anonymity should be respected, unless this prevents the performance of evidence. It must be taken into account that an anonymous complainant could be in a difficult position and that the risk of a potential conflict with the controller could leave him with little options. Given these facts, the Office does not strictly require identification of the complainant which, pursuant to the Article 37 of the Act No. 500/2004 Coll., the Code of Administrative Procedure, includes his name, surname, date of birth, place of residence or other delivery address. According to the findings of the Office, administrative authorities do not fully apply this provision in their practice with respect to the date of birth. The Office bases its considerations particularly on the contents of the petition and, if the contents raise justified suspicion of violation of the Personal Data Protection Act, it applies its supervisory competence (naturally, without the possibility of informing the complainant of the manner of resolving the complaint). Clearly, the right of the parties to peruse files and request copies of written materials, which is based on the entire legislation, cannot be questioned. The fact that the legislation is again not entirely clear in this respect is documented by the following example:

The mother informed the Police of the Czech Republic that she and her daughter had received threats through SMS messages and that they were afraid. The police bodies notified her that if she lodged a criminal complaint and the offender were found, he would become a party to the proceedings and would be able to ascertain even those facts concerning them that he had not previously known. Consequently, the complainant asked the Office that it lodge the criminal notice on her behalf.

Overall statistical data

8 000 telephone inquiries were handled, 41 major personal consultations were provided primarily to Ministries, other public administrative bodies and municipal governments, financial institutions and economic entities (this does not include personal meetings with complainants intended to supplement their petitions), and 1 413 requests sent by electronic mail were answered in 2006.

The following survey documents the categorization of the overall number of 1 889 written petitions according to the affected controllers or processors of personal data:

	inquiries (related to)	justified petitions (against)	justified complaints (against)
Safety and justice	28	22	9
Czech Post	9	9	4
Cooperatives	28	8	7
Transport	13	14	12
Economic entities	331	65	34
Financial institutions	33	31	18

Natural persons	65	34	3
Internet	143	29	1
Mass media	41	16	13
Schools	66	6	7
Telecommunications	54	41	16
Public administration	175	67	20
Health care	53	13	14
Other	270	45	22
T O T A L	**1 309**	**400**	**180**

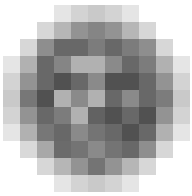
Statistical data on complaints handled in 2006

Petitions
- total ---------- 476
  of which:
  - submitted for inspection ---------- 162
  - submitted for proceeding commencement ---------- 18
  - forwarded to the competent bodies ---------- 3
  - suspended with notification ---------- 293

The number of handled complaints increased by 53 % compared to 2005 (311). The number of 379 accepted complaints is comparable with 2005 (408), as is the percentage share of manners of handling the complaints. This again proved the new role of the Department of Complaints and Consultations, which resolved a number of cases to the satisfaction of the affected entity before any complaint was submitted, i.e. within the provided consultations and legal opinions on the specific issues. A major role was played in this respect by qualified advices provided to citizens and other entities as to how they should proceed in this matter, also outside the regime of the Personal Data Protection Act and the acts directly related to this subject. In addition to the recommendation to thoroughly exercise the rights given to the data subjects particularly by the Articles 12 and 21 of the Personal Data Protection Act and request that the controller provide information or explanation, or correct, block or destroy the processed personal data, the citizens were also advised to resolve their case through a civil lawsuit, exercising their rights in pending criminal or court proceedings, etc.

In the long term, almost two thirds (62 %) of complaints are set aside as unjustified. It is also important that submission of a complaint is not connected with any financial expenses (except the actual cost of submitting the petition). This often results in the fact that complaints are lodged without previously reconsidering the suitability of this approach, e.g. as an immediate response to intense interpersonal relations. Complaints were most frequently designated as unjustified due to the fact that personal data processing was not involved or that personal data were processed in accordance with special generally binding legal regulations.

In conclusion, it can be stated that public awareness of the existence of the Office and its supervisory competence is constantly increasing. Requests for assistance are also lodged by citizens permanently residing abroad. Controllers and processors of personal data also increasingly take advantage of the provided consultations, where it is particularly positive that they use this option as a precaution, in order to avoid any conflict with the Personal Data Protection Act.



Administrative Punishment

1. GENERAL PART

Two substantial changes were made in 2006 in the area of discussion of misdemeanors and other administrative offences by the Office. Probably the most important was the Act No. 500/2004 Coll., the Code of Administrative Procedure, i.e. a brand new regulation of procedures of public administrative bodies that was adopted after more than 40 years of effect of the "old" Code of Administrative Procedure. Any change in procedural, and thus often solely administrative, practices of the public administrative bodies is very demanding from the viewpoint of their employees, the more so where the competent administrative body can infringe on the rights of entities, in relation to which it exercises its powers, as in the case of the Office when it imposes a fine of several millions on a data controller.

On the other hand, the Office has an undoubtable advantage. Indeed, it is a very young administrative body, which has dealt with administrative punishment for "only" 4 years. Thus, it is much easier for it to change its habitual procedures and flexibly adapt to the new legal regulation in the interest of increasing efficiency and quality of its activity results. Increased involvement of the Office's inspectors in this activity, which is the other fundamental change in the area of administrative punishment in 2006, should facilitate the aforementioned objective.

Before the new Code of Administrative Procedure came into effect (January 1, 2006), the employees of the Office had undergone a number of professional training courses aimed at increasing their qualifications in this area. These included workshops concerned exclusively with the specific features of administrative activities of the Office (not only in the area of administrative punishment, but also e.g. transfer of personal data to third countries). The preparations for the new Code of Administrative Procedure included search for new procedures that could be extremely effective from the viewpoint of the objective of activities of the Office, i.e. guaranteeing the right to privacy and the right to protection against unauthorized personal data processing. An order issued pursuant to Article 150 of the Code of Administrative Procedure has proved to be a very suitable instrument (as also follows from the table at the end of this chapter), particularly in cases of less serious violations of the law and also with respect of violations whose merits are fully documented during the control process. These "summary proceedings" have become popular particularly in relation to punishment of dissemination of unsolicited commercial communications, where responsible persons often admit their fault, as well as the fact that mistakes must be punished. The fact that application of this procedure allows the Office to deal with an enormous number of instigations concerning unsolicited commercial communications within the statutory deadlines is also very important.

In relation to the new area of activities of the inspectors in the field of administrative punishment (i.e. a field that had been provided for by December 31, 2005 by the Department of Administrative Activities) and in order to ensure uniform approach of the Office, the President of the Office issued Guidelines for Use of the Form of Acts of an Administrative Authority, which stipulates binding rules

for the use of the form of acts in proceedings pursuant to the Code of Administrative Procedure. Simultaneously, the activities of the inspectors in the area of administrative punishment should take advantage of their experience in the area of control, including not only precise evaluation of the facts, but also, e.g., evaluation of the amount of penalties based on comparison of the ascertained facts with their practical control findings.

The high quality of the proceedings on administrative offences is also documented by the fact that none of the lawsuits challenging decisions of the Office on commitment of an administrative offence has been successful to date. On the contrary, in 2006, the Supreme Administrative Court confirmed, based on an cassation appeal, that the highest fine to date, equal to CZK 3,000,000, which had been imposed for the absence of measures aimed at ensuring security of data, allowing for unauthorized access to and theft of a recording media containing substantial quantity of data of clients of a Czech insurance company, whereby these data were subject to potential unauthorized processing or other misuse, had been imposed in accordance with the law.

2. SPECIAL PART

In this part, we provide information from several areas that are considered by the Department of Administrative Activities to be topical based on its activities in 2006.

Publication of personal data on the Internet

Publication of various personal data on websites is a very topical issue. Publication of personal data of debtors or citizens whose matters have been discussed by municipal bodies is typical for this issue.

It must be emphasized that disclosure of personal data on a website constitutes their processing pursuant to Article 4 (e) of the Personal Data Protection Act and the entity that discloses personal data in this manner (this need not be the same entity as the administrator and operator of the website) is a personal data controller in the sense of Article 4 (j) of the Personal Data Protection Act. When processing personal data, the personal data controller is obliged to proceed in accordance with the Personal Data Protection Act, i.e. fulfill all duties stipulated therein. The fundamental obligations of the controller include the duty to process personal data only with the consent of the data subjects. Without such consent, processing is possible only in cases where one of the conditions stipulated in Article 5 (2) (a) to (g) of the Personal Data Protection Act is met.

However, the fact that the controller processes personal data on the basis of a certain legal title (i.e. the consent or statutory authorization), does not mean that such data may automatically be published on the Internet. Indeed, the purpose limitation principle specified in Article 5 (1) (f) of the Personal Data Protection Act, i.e. the duty to use data only for the purpose for which they were collected, constitutes another fundamental principle of personal data processing. Thus, e.g., an employer who processes relatively extensive sets of personal data on his employees in full conformity with the law is not authorized to disclose these data on the Internet without further authorization (particularly, without the consent of the affected employees). However, certain information (contact details) may be published with respect to employees whose working tasks include communication with the public; nevertheless, this may be done only to the necessary extent. Another example of excess of the limits of the law lies in publication of the information that, due to non-fulfillment of contractual obligations, a certain person is a debtor, where such contract (or some other agreement) does not include the consent of the giv-

en entity to processing of personal data in this manner (e.g. in the form of a contractual penalty).

Thus, every one who intends to publish personal data on a website must carefully reconsider whether such publication will require the consent of the data subject (i.e. a consent obtained in advance that is free and informed pursuant to Article 5 (4) of the Personal Data Protection Act) or whether one of the aforementioned conditions will be fulfilled (however, based on strict interpretation).

Safeguarding personal data processed within medical documentation

Given the fact, in addition to "normal" personal data, sensitive data in terms of Article 4 (b) of the Personal Data Protection Act are processed within medical documentation (pursuant to Articles 67a and 67b of Act No. 20/1966 Coll., on public health care), it is necessary to adopt and consistently implement due measures within keeping and treatment with this documentation, preventing unauthorized or accidental access to the personal data or their loss.

The duty to adopt such measures follows from Article 13 (1) of the Personal Data Protection Act for the entity that keeps the medical documentation, i.e. the health-care facility (without respect to whether this is a legal person or a natural person who is an entrepreneur). This duty encompasses evaluation of all risks related to the given processing of personal data, based on the specific arrangement of processing and the circumstances under which the processing is carried out, and also adoption and implementation of the corresponding measures. Suitable measures to ensure personal data protection must be adopted, not only in relation to the usual activities of the health-care facility, as the controller or processor of personal data, but also especially for each individual operation involving personal data, or carriers thereof, which exceeds the scope of usual activities of the controller or processor, such as transport of written documents (medical documentation) to some other place, their transfer to some other entities or destruction of materials preserved in archives. When evaluating the risks and adoption of measures in terms of Article 13 (1) of the Personal Data Protection Act, it is also necessary to deal with the risk of theft of the documentation or other carriers, i.e. also personal data which they contain.

Personal data processing in relation to administration of real estate

Administration of buildings, whether they are owned by an association of owners or by a cooperative, always involves processing of personal data of the inhabitants of the building. These data are necessary for proper administration of the building, including management of the repair fund or allocation of joint expenses. This processing may either be carried out by the owner of the real estate (the controller of personal data) or it may be entrusted to some other entity, which then acts as the personal data processor. The responsibility for personal data processing is borne primarily by the controller; however, in case of excess or non-compliance with the set conditions for processing, it is also (or exclusively) borne by the processor.

Processing of personal data collected within administration of a building always requires particularly compliance with the purpose limitation principle expressed in Article 5 (1) (f) of the Personal Data Protection Act, i.e. use of the data only for the purpose for which they were collected. Non-compliance with this principle, i.e. breach of the duty in processing of personal data, may also consist in publication of personal data, e.g. in relation to existence of a debt towards the owner or manager of a real estate, at a place that is also accessible to persons other than those who are entitled to obtain such information based on their membership in the association of owners or the cooperative.

In buildings, where part of the inhabitants are owners of apartments or members of the cooperative and part are tenants of those entities, proper fulfillment of the duties stipulated by the Personal Data Protection Act for administration of the building requires that the position of the individual inhabitants be distinguished. Information (including personal data), to which the co-owners of the building, i.e. those persons who financially contribute, e.g. to management of the common premises or to repairs, are entitled, may not automatically be disclosed to all inhabitants of the building. E.g. a notice that a certain co-owner or member of a cooperative owes contribution to the repair fund or information on the amount contributed by such person to reconstruction of the building may be disclosed to other co-owners and members of the cooperative, but not to tenants; similarly, information concerning the tenants may be disclosed, within an appropriate scope, to other co-owners of the real estate (as, e.g. the number of persons in a household is important for administration of the entire building), but not to other tenants.

Simultaneously, it can be stated that, even if all inhabitants of a building were owners of apartments or members of the cooperative, it would not be suitable to disclose information containing personal data in publicly accessible parts of the building (even if it were locked), as it cannot be ensured that it will not thus be disclosed to other persons, e.g. visitors.

Subject of updating of processed personal data

On the basis of Article 5 (1) (c) of the Personal Data Protection Act, every controller or processor of personal data is obliged to process only accurate personal data and update the processed personal data if necessary. This is closely related to the duty specified in Article 5 (1) (e) of the Personal Data Protection Act, i.e. the duty to preserve personal data only for a period of time that is necessary for the purpose of their processing.

It follows from the above that every one who processes personal data must adopt a system of measures, depending on the scope and circumstances of the relevant processing, whereby he prevents processing of inaccurate or false personal data (i.e. the potential inadequacies in the quality of data shall be ascertained and remedied), as well as preserving of personal data whose processing is no longer required from the viewpoint of fulfillment of attaining the set objective.

It should be noted in this relation that processing of inaccurate personal data pursuant to Article 5 (1) (c) of the Personal Data Protection Act includes, not only processing of incorrect data obtained from unverified sources or following, e.g., from a spelling mistake, but also processing of formally correct data in relation to an incorrect information. This includes, e.g., processing of accurate identification data together with information that the given person is a debtor, although this is not, in fact, the case. Indeed, in terms of Article 4 (a) of the Personal Data Protection Act, personal data shall mean any information that can be related to a specific person.

However, the duty to process only accurate personal data does not mean that it is always necessary to process only absolutely correct data, as inaccuracies can arise already during the collection of data from the data subjects, for which the given controller is not liable. Nevertheless, the Personal Data Protection Act requires that the personal data controller (or the processor, on the basis of the controller's authorization) also update the processed personal data and thus remedy any ascertained inaccuracies, if this is necessary with respect to the purpose of processing. The Personal Data Protection Act does not impose on the controller to perform such control of correctness of the processed data continually, but rather leaves up to the given controller to decide on the manner of dealing with this duty, based on the purpose and means of processing. Thus, measures aimed at as-

certaining processing of incorrect personal data are necessary particularly within systems whose operation is fully or substantially automated and that are intensively utilized.

The finding that inaccurate or redundant personal data are being processed is often made on the basis of a request of the data subject for correction, supplementation or liquidation of the processed data. It must be stated that, on the basis of Article 21 of the Personal Data Protection Act, the controller is obliged to satisfy such request of the data subject (if justified).

Processing of birth numbers

As of April 1, 2004, special regulation of use of birth numbers has been incorporated in Act No. 133/2000 Coll., on register of population and birth numbers and on amendment to some acts (Register of Population Act), whose Article 13c (1) stipulates an exhaustive list of cases when birth numbers may be used. Given the fact that, in spite of their special status, birth numbers are personal data in terms of Article 4 (a) of the Personal Data Protection Act, the Register of Population Act is a lex specialis to the Personal Data Protection Act. Thus, every person who processes birth numbers is a personal data controller pursuant to Article 4 (j) of the Personal Data Protection Act and is subject to all duties imposed by the Act, unless the Register of Population Act stipulates otherwise.

In the private sphere, birth numbers may be used primarily only on the basis of the consent of their holders, i.e. pursuant to Article 13c (1) (c) of the Register of Population Act. Indeed, Article 13 (1) (a) of this Act grants authorization to use birth numbers only to State administrative bodies listed therein and only for the procedure pursuant to Article 13c (1) (b) of the Register of Population Act, i.e. use of the birth number, where stipulated by the special act, requires that the special act explicitly stipulate the duty to identify the parties to a certain legal relationship by birth numbers.

However, birth numbers are still often used by entities of private law (such as legal counsels) to designate the parties to a court dispute or parties to proceedings or this data is directly required by the competent State authorities. Nevertheless, this is absolutely inacceptable, as the Register of Population Act or some other regulation authorizes directly only just State institutions to obtain and utilize birth numbers. On the contrary, the individual parties to the dispute or their counsels are thus de facto forced to process birth numbers at variance with the law, as only exceptionally will the plaintiff be able to obtain the consent to processing of the defendant's birth number and the legal regulations usually do not permit processing of birth numbers by private-law entities.

E.g., Article 79 (1) of Act No 99/1963 Coll., the Code of Civil Procedure, does not stipulate the duty to identify the parties to the court proceedings (natural persons) by birth numbers and merely requires that the proposal for commencement of the proceedings contain, in addition to the general requisites, the name, surname and place of residence of the parties. It follows from the above that Act No. 99/1963 Coll. is not a special act in terms of Article 13c (1) (b) of the Register of Population Act, allowing for use of birth numbers. The authorization to use birth numbers for identification of defendants also cannot be derived from the fact that some public registers that are accessible by remote access (e.g. the Land Registry and the Commercial Register) contain birth numbers and thus disclose them to the general public. While processing of birth numbers in relation to keeping of these registers can be considered inappropriate from the viewpoint of the principles of protection of personal data and privacy, it is in accordance with Article 13c (1) (a) of the Register of Population Act. However, the relevant legal regulations stipulating the conditions for operation of these registers do not au-

thorize the users to freely dispose of the birth numbers specified in the registers.

In conclusion, it should be stated that the consent to use of the birth number pursuant to Article 13c (1) (c) of the Register of Population Act means, given the absence of a special regulation, consent to processing of personal data pursuant to the Personal Data Protection Act, i.e. free and informed manifestation of will preceding the actual processing.

3. IMPOSED PENALTIES

In this part, we concentrate on 5 most important cases of breach of duties in personal data processing – based on the amount of imposed penalty.
N.B. : Only proceedings on administrative offences that were validly completed in 2006 were included in this part

The highest fine imposed within the competence of the Office pursuant to the Personal Data Protection Act was imposed last year on a **church** that failed to inform its members and applicants for membership in relation to collection of their personal data of the scope and purpose for which the personal data would be processed, by whom and in what manner they would be processed and to whom the personal data could be disclosed, and on the right of access to his/hers personal data, on the right to correction of personal data and on other rights pursuant to Article 21 of the Personal Data Protection Act. Simultaneously, it failed to advise them as to whether the provision of personal data was obligatory or voluntary. Furthermore, this church, which also processed sensitive data related to its members (e.g. information on religion), disclosed their personal data without their consent on its website and in its monthly bulletin and, furthermore, provided them without the consent of the affected data subjects to two business companies based on an agreement on provision of public relations and an agreement on provision of consultancy. At variance with the Personal Data Protection Act, this church also inadequately and partly also indemonstrably adopted and documented technical and organizational measures to secure personal data protection, and the actual state of affairs did not correspond to those measures. Through the above-described conduct, the church breached the duties stipulated in Article 9 (e), Article 11 (1) and (2) and Article 13 (2) of the Personal Data Protection Act, for which the first-instance body of the Office imposed a fine of CZK 300,000. On the basis of an remonstrance, within the appellate proceedings, the President of the Office confirmed the factual and legal conclusions in the contested decision; however, given the circumstances, under which the administrative offence was committed, particularly with respect to the mission of the church, he resolved to **reduce the imposed fine to CZK 150 000**.

Another high fine was imposed by the Office on a **hotel operator**, whose employees, namely hotel receptionists, acquired copies of personal documents of the guests over a period exceeding four years. A copy of the identification card contains personal data including the name, surname, date of birth, birth number, sex, place of birth, nationality, signature and photograph of its holder, the number of the identification card and its validity. In cases where a copy was made of the reverse side of the identification card, the hotel operator also collected other personal data including the address of residence, maiden name, place of birth and family status. The aforementioned copying of personal documents breaches several provisions of the Personal Data Protection Act; primarily, the hotel thus collected personal data that did not correspond to the specified purpose, i.e. protection of

guests and their property, and did so within a scope that was not necessary for fulfillment of the specified purpose. Given the fact that the copies were preserved for the entire period of the above-described illegal conduct until the Office's inspection, personal data were also preserved for a period longer than required for the purpose of processing. At the same time, the hotel operator failed to obtain the consent of the guests to such processing of their personal data, although the aforementioned collection of personal data is not subject to any of the exemptions pursuant to Article 5 (2) of the Personal Data Protection Act. Thus, the aforementioned conduct constituted breach of the duty pursuant to Article 5 (1) (d), Article 5 (1) (e) and Article 5 (2) of the Personal Data Protection Act, for which the Office imposed a **fine of CZK 100 000**.

The Office also imposed a high penalty on a **business company**, whose employees handled forms and other documents (such as applications for the provision of telecommunication services by a mobile operator, copies of identifications cards, cash receipts) at variance with the principles of protection of personal data and privacy, as they failed to destroy or otherwise suitably liquidate the aforementioned documents, but rather only placed them near waste containers, whereby they made accessible personal data of 78 customers of the mobile operator including their name, surname, address of residence, date and place of birth, sex, birth number, telephone number, nationality and signature. Thus, they breached the duty stipulated in Article 13 (1) of the Personal Data Protection Act, even though the company had adopted the Principles of Processing and Protection of Personal Data, as the employee who committed the aforementioned conduct had not been acquainted with those rules and, thus, it was clear that these principles were merely declaratory, but were not incorporated in the company's common practice nor subsequently controlled. For the aforementioned breach of the duty pursuant to Article 13 (1) of the Personal Data Protection Act, the Office imposed a **fine of CZK 100 000**.

Another penalty was imposed on a **statutory broadcaster** in relation to processing of personal data of natural persons, payers of the television fee. At variance with the Personal Data Protection Act, the statutory broadcaster kept register of payers of the fee including inaccurate personal data and failed to update these personal data within the necessary scope. Indeed, the duty to process only accurate personal data, which is expressed in Article 5 (1) (c) of the Personal Data Protection Act, cannot be construed in that the personal data controller is obliged to take a remedial measure only when he ascertains that the personal data which he processes are not accurate with respect to the specified purpose; rather, it is always necessary to apply the full wording of the provision of the law, i.e. including the second sentence, which stipulates the duty to update the processed data. The manner and frequency of updating must be set by the personal data controller himself, particularly with respect to the purpose of processing, the character of the records and the manner of their use. As the statutory broadcaster failed to duly fulfill the above-specified duty, he breached the duty stipulated in the given provision of the Personal Data Protection Act, for which a **fine of CZK 100 000** was imposed.

4. TABLE

Number of instigations concerned with a suspected administrative offence pursuant to the Personal Data Protection Act and the Register of Population Act

Total 61
of which – on the basis of control activities of the Office 20
– by referral of the matter by the prosecuting bodies 11
– on the basis of an instigation from natural and legal persons 30
Settled:*
– through a decision on imposing a fine (total) 43
of which through an order 8
– other decision (e.g. suspension prior to commencement of proceedings, discontinuation of proceedings, decision that an offence has not been committed) 19

* *Including settling of instigations, whose discussion was commenced in 2005*

5. ADMINISTRATIVE PROCEEDINGS PURSUED BY INSPECTORS

As mentioned above, a major change was made in 2006 with respect to the pursuit of administrative proceedings by officially authorized employees of the Office; proceedings may newly be pursued by the individual inspectors of the Office. Within the pursuit of administrative proceedings and preparation of a first-instance decision on imposing a penalty and specification of its amount, they are able to take greater account of specific findings from their inspections. Within this activity, the inspectors utilized particularly the institute of summary proceedings following after completion of the inspection, which provides a possibility of effectively reducing the length of the entire proceedings and, simultaneously, allows the parties to these proceedings to utilize all options associated with this institute.

In 2006, the inspectors of the Office performed a total of 116 administrative proceedings, of which vast majority, 107, were undertaken in the form of an order pursuant to Article 150 of the Code of Administrative Procedure. This procedure is employed particularly in relation to unsolicited commercial communications (over 80 % orders), but it is also used in proceedings on other violations of the Personal Data Protection Act.

Administrative proceedings pursued by the inspectors due to violation of the personal data protection yielded the following results.

Commenced were: 27 proceedings not concerned with unsolicited commercial communications.

Appeal was not lodged against any decision; protest was lodged against 6 orders.

Final decision was issued in 2006 in: 100 proceedings.

The highest fine was imposed on a private health-care company and its amount equaled CZK 150 000.

6. SECOND-INSTANCE PROCEEDINGS AND COURTS

In 2006, the second-instance proceedings were affected by a change in the legal regulations, both in relation to the new Code of Administrative Procedure and in relation to amendment to the Act on State Inspection brought by Act No. 501/2004

Coll., which modified the proceedings on objections that had been previously applicable. Thus, a decision is always made in the second instance on objections against the inspection protocol in cases where the person performing inspection does not satisfy the objections. The proceedings then result in a decision of the President of the Office, which is final and, where the circumstances so indicate, becomes a basis for commencement of administrative proceedings on imposing a penalty. Objections of the controlled person thus become one of the bases for issuing a decision. By omitting the redundant "level" of decision-making by the inspector in control proceedings (on objections against the protocol) and by omitting an appeal against the inspector's decision on objections against the protocol – the control proceedings which also include proceedings on objections against the protocol were approximated with the administrative proceedings, resulting in a substantial increase in effectiveness of the activities of the Office and in releasing the inspectors' capacity.

In 2006, the President of the Office made ten decisions on objections. It can be summarized that, in almost all cases, the controlled entities raised objections against the same mistakes of the inspectors. Objections were lodged against incorrect legal assessment of the matter, incorrect assessment of the established facts of the case or incorrect control procedure. In this relation, in several cases, the controlled entities also claimed that the imposed remedial measures be cancelled. It must be noted that, in certain cases, the President acknowledged the arguments of the controlled entities, as follows from the table below. In two of those cases, the remedial measures were partly or fully cancelled.

Objections	**Number**
Accepted	5
Partly accepted	2
Dismissed	3
Total	10

As follows from other parts of the annual report, the Office pursued a number of administrative proceedings on the basis of the results of the inspections, as well as on the basis of other facts ascertained within the supervisory activities, where such proceedings were completed by imposing a penalty.

As stipulated by the Code of Administrative Procedure, such decisions are subject to remonstrance, which is a special form of a remedy set out by the law (the Code of Administrative Procedure) for cases where the decision in the first instance was issued, *inter alia*, by a central administrative authority, which certainly is the case in relation to the Office for Personal Data Protection, in terms of Article 2 (2) of the Personal Data Protection Act.

A decision on the remonstrance is then made by the President of the Office on the basis of a proposal submitted by a remonstrance committee established by the President, which worked in enlarged and modified membership in 2006. The appellate proceedings were also modified based on the new regulation of administrative proceedings. While this regulation made no principal changes to the previous legal state of affairs, it somehow raises doubts about the manner, in which the President of the Office may make decisions on remonstrance. Opinions prevailed in practice that the President may make a decision on an remonstrance in that he dismisses it and upholds the challenged decision, or changes the decision of the first-instance body or, if he finds statutory grounds, he may also cancel the first-instance decision.

In 2006, the President of the Office made decisions on remonstrance in a total of nineteen cases. It can be stated that the reasons for lodging a remonstrance cor-

responded to a substantial degree with the reasons, due to which objections were lodged within control proceedings. Thus, these reasons again involved incorrect legal assessment of the matter, incorrect assessment of the established facts of the case based on inadequate evidence. The actual competence of the Office to pursue the proceedings was questioned and arguments were also made with respect to nullity of the issued decision, bias or inappropriate amount of the imposed penalty. Through their remonstrance, practically all the individual entities claimed that the first-instance decision be cancelled or that it be found that the given act had not been committed, or they requested that the penalty be reduced. The overall results of decision-making are given in the following table, which is classified according to the basic characteristics of the decision on remonstrance.

First-instance decision	**Number**
upheld (remonstrance dismissed)	14
cancelled (remonstrance accepted)	3
changed (remonstrance partly accepted)	2
Total	19

In accordance with Article 4 (1) (a) of Act No. 150/2002 Coll., the Code of Administrative Justice, as amended, courts make decisions within administrative justice on actions against decisions issued by "administrative bodies" in the area of public administration. Entities on which the Office has imposed penalties within administrative proceedings for violation of the Personal Data Protection Act or of some other law, under which the Office is authorized to impose penalties, use the option of lodging an administrative action relatively frequently.

It can be stated that the number of cases where the decision of the Office is challenged by an administrative action has been relatively stable and has not changed in absolute values compared to the previous years. A total of 14 court disputes are currently pending; however, within this number, some cases have been completed and new court disputes have been initiated. Courts have resolved four disputes during the year. The decisions were mostly favorable for the Office. In one case, the court discontinued the proceedings as the action had been withdrawn. In two cases, the Municipal Court in Prague upheld the Office's decision and dismissed the action. Both decisions were then contested by the counterparty through a cassation complaint; in one case, the Supreme Administrative Court dismissed the cassation complaint and the other case was returned to the Municipal Court for new proceedings. In one case, the Municipal Court cancelled the relevant decision of the Office and returned the case for further proceedings.

The decisions of the Office on imposing a penalty were challenged by an administrative action in four other cases in 2006. However, a decision has not been made on these actions to date.

7. COMPLAINTS HANDLING LODGED PURSUANT TO ARTICLE 175 OF THE CODE OF ADMINISTRATIVE PROCEDURE

As mentioned in the related parts of the Annual Report, an important role in application of the new regulations in 2006 was played by the new Code of Administrative Procedure (Act No. 500/2004 Coll.), including new Article 175 dealing with complaints. Pursuant to that Article, the affected persons have the right to lodge with administrative bodies complaints against unsuitable behavior of officials or against the procedure of an administrative body, unless this Act provides for some other remedy. Lodging a complaint must not lead to any harm to the com-

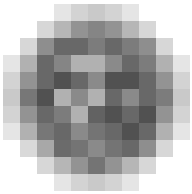
plainant; liability for a criminal offence or administrative offence is not prejudiced by this provision.

A complaint may be lodged in writing or orally; if a complaint is lodged orally and cannot be dealt with immediately, the administrative body shall make a written record thereof.

A total of 18 persons lodged complaints with the Office in 2006 based on this new provision. In twelve cases, the complaints were evaluated as unjustified, in three cases as justified and in three cases as partly justified.

The President of the Office established a special working procedure for dealing with these complaints, which were often aimed against control findings of the inspectors (in 5 cases); under this procedure, it must be reviewed as to whether the employee of the Office, against whom the complaint is directed, used all possibilities for dealing with the matter that is subject to dispute. No complaint was lodged against the behavior of the employees of the Office, which is a good sign, as the process of resolving instigations within the inspection or administrative process is not always straightforward.

All complaints were resolved within the statutory deadline. Three cases, where the complaint was found to be justified, particularly those cases where it was directed against the result of assessment of a complaint or instigation concerned with illegal processing of personal data, with the contents of which the complainant had disagreed, were submitted to an inspector for control.



Activities of the Office in the Legislative Area

AMENDMENTS TO THE PERSONAL DATA PROTECTION ACT

Act No. 101/2000 Coll., on personal data protection and on amendment to some acts, was affected only by minor changes in 2006, after the previous fundamental revisions. Based on the more accurately defined procedure in the provision of data from the information system of the register of population pursuant to Act No. 133/2000 Coll., on register of population and birth numbers and on amendment to some acts (Register of Population Act), the Office was authorized to use certain part of data from these records for the performance of its competence. The modifications made in Article 9 of Act No. 101/2000 Coll. reflect the newly adopted regulations in the area of social services and accident insurance, which involves processing of sensitive data.

AMENDMENT TO THE ACT ON CERTAIN SERVICES OF THE INFORMATION SOCIETY

A fundamental change was made in **Act No. 480/2004 Coll., on certain services of the information society** and on amendment to some acts (the Act on Certain Services of the Information Society), under which the Office performs supervision in relation to unsolicited commercial communications. With effect from August 1, 2006,

new rules apply to the use of electronic contact data obtained in connection with the sale of products or services for dissemination of commercial communications on one's own similar products or services, based on the opt-out principle. Thus, the original rules were replaced by less restrictive legislation that is more favorable for business. This change had been repeatedly proposed by the Office, as it follows from the requirements of the EC law and reflects the general rules concerning protection of privacy (for more details on this aspect, see p. 27).

NEW COMPETENCE OF THE OFFICE

The new legal regulations adopted in 2006 confirmed that the Office, as a supervisory institution dealing with personal data processing based particularly on its control findings, can effectively discuss various infringements on public interests that have been previously detected by it and, therefore, the Office has been provided with competence to discuss misdemeanors and other administrative offences for special areas of personal data processing.

According to the **amendment to Act No. 329/1999 Coll., on travel documents** and amending Act No. 283/1991 Coll., on the Police of the Czech Republic, as amended (the Act on Travel Documents), with effect from September 1, 2006, the Office has been the competent authority in the first instance in procedures on misdemeanors and administrative offences consisting in illegal processing of data on data carriers with biometric data.

With effect from January 1, 2007, new legislation will govern the conditions related to limitation of certain activities of public officers and the incompatibility of the position of public officer with other positions. These provisions are contained in **Act No. 159/2006 Coll., on conflict of interests**, which constitutes a new area of personal data processing and, amongst other things, also stipulates the punishment for misdemeanors discussed by the Office, consisting in improper treatment with information from the register of notifications submitted by public officers on their activities, notification of property and notification of income, gifts and liabilities.

LEGISLATIVE PROCESS AND COMMENTS ON LEGAL REGULATIONS

In the area of provision of comments on legal regulations, it can be stated that, *based on implementation of the EC law* in the legislation of the Czech Republic, the *principles of personal data processing have been more consistently reflected* in the preparation of new bills. This makes even more marked the "autonomous" areas of national law that are still unaffected by these higher principles, particularly the areas of administrative agenda, where official procedures are inadequately defined, which leads to purposeless keeping and often further unlimited processing of personal data by the State administration. In this relation, within its comments on draft legal regulations concerned with the aforementioned areas, the Office has dismissed the mere declaratory references to compliance with the principles of personal data protection and rather insisted on specification of accurate procedures in processing of personal data, particularly where different variants of processing or justified exemptions from the standard procedures are proposed.

In 2006, within discussion of drafts implementing regulations, the Office also noted the *need for further specification of rules*, particularly for preserving, providing and publishing personal data within the Commercial Register and the Land Registry. It also proposed a substantial revision of implementing and other related regulations that were amended in 2006 with respect to inappropriate processing of personal data and the excessively regulatory legislation within procedures employed in schools pursuant to Act No. 561/2004 Coll., on preschool,

elementary, secondary, higher vocational and other education (the Act on Schools).

In relation to evaluation of the experience with application of Act No. 101/2000 Coll., the Office further *emphasized the need for rules of protection of privacy also in areas that are not directly subject to Act No. 101/2000 Coll.* It based its considerations, *inter alia*, on the results of analyses and binding EU documents, which unambiguously state that adequate rules must be stipulated for personal data processing also in case of certain special subjects. These subjects include, e.g., security aspects, which have been exempted to date from the scope of Act No. 101/2000 Coll. – the provisions concerning the Schengen Information System, which are currently being prepared, will be fully governed by the aforementioned law. More specific EU "sectoral" protection of personal data in the area of security can be expected in the near future.

Another problematic area monitored and evaluated by the Office includes *prevention of risks in personal data processing and prevention of their misuse*, which is always connected with application of Article 13 of Act No. 101/2000 Coll., which imposes on the controller and processor the obligation to adopt measures preventing unauthorized or accidental access to personal data, their change, destruction or loss, unauthorized transfers, other unauthorized processing, as well as other misuse of personal data. Thus, the Office has accepted the arguments of controllers and processors, as well as of the professional public, who, on the one hand, believe that the relevant provision is difficult to apply in some cases and, on the other hand, consider it inadequate in the current general form. The Office proposed specific procedures that should supplement the general framework delimited in Article 13 of Act No. 101/2000 Coll. and some special cases of personal data processing, particularly in the area of automated processing of data.

The Office noted with satisfaction that, together with other ideas, it was able to apply the aforementioned approaches *in cooperation with those institutions*, whose competence includes submission of draft regulations and which showed interest in consulting certain aspects, not only within the relatively short period of providing comments on draft regulations, but also sufficiently in advance within preparation of information justifying the need for amendment to legal regulations or preparation of a substantive intent of a law. Thus, cooperation was developed in 2006 within tasks concerning, e.g., reflection of the Schengen acquis in the Czech legislation and preparation of the draft design of future nationwide statistical censuses.

This approach implements Article 20 (3) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which contemplates that, for processing that could pose special risks from the viewpoint of rights and freedoms of the affected persons, *checks should be performed in the context of preparation either of a measure of the national parliament* or of a measure based on such a legislative measure.

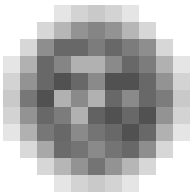
Unfortunately, experience of the Office to date has also showed unwillingness of some authors and parties submitting drafts of acts to find such a form of a legal regulation and arrangement of legal relations that would respect the rights and freedoms guaranteed by the Constitution and to strive to *find a balanced relation between the citizen's right to privacy and the right for safeguarding other interests that could limit the citizen's privacy to the necessary degree.*

One of the unfavorable examples was related to the problematic manner of performing the background check in the area of civil aviation. This check was based on the need to comply with the requirements following from Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security; a total of

14 000 persons in the Czech Republic had to undergo the check. The Office could not perform effective inspection in this case, as the verification was carried out in accordance with the newly adopted Czech legal regulations; however, on the basis of doubts following from legal assessment of the given subject, it requested its repeated and consistent analysis. The Office expressed its doubts as regards purposefulness and proportionality of personal data processing, i.e. doubts concerning the need to apply a uniform regime of verification to all affected persons, as already Regulation No. 2320/2002 required that the relevant detailed implementing measures in the regulated areas be appropriately adapted to each activity and sensitiveness of certain measures. It was also noteworthy that the new area of personal data processing and the specific obligations following therefrom were actually established only as a consequence of promulgation of a secondary legal regulation, consisting in no longer valid today Regulation of the Government No. 31/2005 Coll., laying down the list of sensitive activities for civil aviation, furthermore, without proper evaluation of the impact of the set solutions on the privacy of the affected persons. Remedy in the relevant matter was attained by adoption of Act No. 225/2006 Coll., amending particularly Act No. 49/1997 Coll., on civil aviation.

While the first case *shows inadequacies of the legislative process* at the level of State administration, the second example relates to the end of this process. The Parliament discussed draft Act to amend Act No. 266/1994 Coll., on railways. Although this was repeated discussion of a draft legal regulation, it is surprising that, in one of the final stages of its approval, without consulting the entities engaged in protection of personal data and without any opinion from the sectors responsible for transport aspects and the information system of the register of population, it was proposed that access of private entities be allowed to a register intended for the needs of the public administration. The proposed authorization of transport operators was justified by the attempt to allow for prosecution of persons evading payment of traffic fares and to allow the transport operators to request supplementation or specification of personal data from the information system of the register of population for the purposes of submitting a proposal for commencement of proceedings on payment of the traffic fare (and the surcharge). However, the wording of the draft was clearly formulated without respect to the long-prepared amendment of the Register of Population Act concerning specification of the rules for withdrawal and use of data from the register of population, which was discussed in the Parliament at the same time. From the viewpoint of the rules of personal data processing, the new authorization of the transport operator to withdraw data from the register of population was unjustified, as it did not ensure that actual data on a specific passenger would be ascertained, furthermore, in a situation where, pursuant to the applicable regulations, transport operators could use other appropriate statutory means to exact traffic fares and, particularly, to ascertain the true identity of dishonest passengers. Admittedly, the adopted draft does not resolve the most frequent behavior of non-paying passengers, who provide personal data of other persons upon control in transport. The Office provided a dissenting opinion on a similar draft supplement to Act No. 111/1994 Coll., on passenger transport, and Act No. 266/1994 Coll., on railways, in 2001.

With respect to the aforementioned cases, the Office strived in 2006 to provide for creation of preconditions for standard assessment of draft legal regulations also from the viewpoint of impact on the privacy of citizens within the entire legislative process. We can only hope that the activities of the *Standing Commission for Protection of Privacy that was established in the Senate in November 2006* will contribute to this goal.



Registration

The activities of the Registration Department in 2006 were concerned particularly with creation of a new web application of the register allowing the controllers to provide notifications of personal data processing by electronic means. The goal was particularly to accelerate and streamline the entire registration process and to simplify the fulfillment of the registration duty by the controller by creating an electronic form.

First, it was necessary to modify the registration forms. The registration forms that had been available only on paper at selected tax authorities were used by almost 99 % of all controllers to fulfill the notification duty. Only rarely had the controllers chosen an alternative means of lodging the notification by mail. Therefore, it was necessary to pay due attention to their modification. Given the several amendments to the Personal Data Protection Act which also affected the contents of the registration process, it was necessary to further specify and supplement the registration forms so that they corresponded to the applicable legal regulations. In particular, the new design of the registration form includes all information necessary for assessment of the given notification from the viewpoint of the risks associated with the intended processing and, thus, better suits the needs of the Office with respect to further performance of the supervisory activities. One of the main changes in the registration form was related to the manner how the controller notified the Office of the purpose of processing. Each processing of personal data is characterized particularly by its purpose. Therefore, the actual assessment of the lodged notification requires that the purpose or purposes of processing be clearly and comprehensibly defined. Through the form, the administrator is invited to provide brief description of the processing of personal data.

Another change was concerned with the manner of fulfillment of the notification duty by the controllers. In the interest of ensuring greater comfort of the notifiers (the controllers), facilitating and modernizing communication with the citizens, a change was made in the technical processing of the forms, taking also account of the interests of applicants that had been ascertained by the Office. Naturally, the transfer to the web application (electronic form) resulted in the need for creating an entirely new information system of the register, allowing for acceptance and processing of registration notifications that were filed electronically. Again, the task of creating a new information system was entrusted to an external firm.

Thus, from November 27, 2006, the controllers may lodge registration notifications electronically through the form located on the Office's website at www.uoou.cz in the section "Register". The electronic form also includes detailed instructions for its completion. After filling in all the required items, the notifier sends the form electronically and the system informs him by means of a short notice of successful dispatch. In terms of the Act, the controller is authorized to commence processing of personal data on the date of registration in the register or after expiry of the statutory deadline, i.e. after 30 days from the date when the notification of the processing was delivered to the Office, unless the controller has been invited to supplement the notification and unless administrative proceedings have been

initiated on reviewing the legality of the notified processing of personal data pursuant to Article 17 of the Act.

The original registration forms that had been available at selected tax authorities have been withdrawn from circulation. The new registration form is no longer available in printed form. However, it can be printed from the Office's website and sent by mail or filled in and sent electronically. The controller may also choose to fulfill the notification duty without using the form. In this case, it must be ensured that the petition contains all the information required by law.

More than a month of operation of a new electronic registration form can be evaluated very favorably from the viewpoint of functionality of the system, fulfillment of expectations and the benefits both for the Office and for the controllers. It appears that the controllers have become used to this manner of filing registration notifications and, at the same time, welcomed its simplified design. This is documented by 240 new registration notifications lodged during the last month, which corresponds to an increase by approx. 100 % compared to the monthly averages over the entire year. Practically from the first day of operation, the Office has been receiving dozens of new notifications. Fears that the controllers would continue to lodge notifications on old forms did not prove true (this occurred only in a few cases). It is also positive that we almost never encounter any inquiries indicating problems with filling in the form or other irregularities (the overall comprehensibility of the form for the controllers was one of the main priorities). In contrast, it can be stated that the controllers often use the possibilities of the new form and provide the Office with detailed information on the contemplated processing, particularly description of the actual purpose of processing. This facilitates, *inter alia*, closer contact with the controller and often also subsequent telephone or oral consultations concerning the notified processing, which should ensure that the processing is in conformity with law. Simultaneously, this fulfilled the expectation of the Office that the new registration forms would enable it to obtain more comprehensive information on the notified processing, allowing it, *inter alia*, to fulfill its statutory duty more effectively, i.e. to ascertain and verify any cases of processing that could be at variance with law.

The trend of gradual decrease in the number of notified cases of processing in the previous years has ceased this year. Compared to 2005, the year 2006 witnessed an increase in the number of registration notifications by approx. 40 % (see the table), which was caused particularly by the high number of notified cases of processing of data by means of a video surveillance system. A positive feature consisted in the reduced number of proceedings suspended due to the fact that processing was notified by the processor (the registration duty applies only to controllers) or due to the fact that processing was notified although it was not subject to the notification duty and its registration in the register was thus unjustified. While in 2005 this occurred in approx. 35 % of the total number of notifications lodged with the Office, in 2006 this ratio equaled only approx. 14 %. From time to time, the Office publishes on its website comments concerning various types of processing that are not subject to the notification duty. The main reason for this approach lies in the opinion, which had been very common until recently, that each case of processing of personal data must be notified to the Office. Continuous provision of information to the controllers contributes to correcting this opinion and, thus, the Office is able to pay more attention to verification of the high-risk types of processing.

One of the main objectives of the registration proceedings is to detect cases of processing that could be at variance with the law or processing that could pose special risks from the viewpoint of the rights and freedoms of the data subject. Admittedly, assessment of the given case of processing requires adequate and accu-

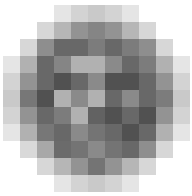
rate information. The new, or rather modified, registration form capable of providing this information should be a milestone in this respect. The registration proceedings relatively frequently result in the controller modifying the contemplated processing (e.g. the controller resolves not to process sensitive data). This *de facto* prevents illegal procedures in processing of personal data prior to actual commencement of the processing. However, the controllers often address the Registration Department with a request for consultations prior to lodging a written notification of processing. This involves particularly advice on the actual nature of processing, specification of its purpose, proportionality of personal data processed with regard to the declared purpose, duties of the controller in processing of sensitive data, the conditions for transfer of personal data abroad, etc. Thus, the Registration Department is substantially involved in the overall raising of awareness of the controllers of the rights and duties in personal data processing.

The year 2006 witnessed an enormous increase in the number of notified cases of personal data processing by means of video surveillance. In January 2006, the Office issued a written position on the subject of video surveillance systems, which also contained the main principles of operation of a video surveillance system from the standpoint of the law. Under certain circumstances, the operation of a video surveillance system can constitute personal data processing in terms of the law and thus controllers have, amongst other things, the duty to notify the Office of this processing through the procedure pursuant to Article 16 of the Act. However, this fact has not yet been sufficiently acknowledged by the general public. In 2006, approx. 390 controllers operating video surveillance systems applied for registration, which is a substantial increase compared to previous years (about 5 controllers were registered in 2005). On the other hand, this is still quite a small fraction compared to the actual number of video surveillance systems installed in the CR, which are being increasingly used in schools, museums, residential buildings, banks, retail chains, etc. Registration notification lodged by a financial institution documents the scope of use of video surveillance systems in this country. The institution notified the Office of installation of video surveillance systems in all its approx. 750 branches, which involves thousands of installed cameras.

In relation to installation of a video surveillance system, it is always necessary to thoroughly consider whether the specified purpose (protection of property, prevention of vandalism, etc.) could be attained by other means or procedures. Video surveillance must not excessively infringe on privacy. In this sense, the Office has recorded several notifications where the controller (operator of the video surveillance system) intended to display the monitored area (public areas, store, internet coffee shop) on-line on the internet. Controllers frequently notify the Office by means of the registration notification of their intention to process the personal data of employees through video surveillance for the purpose of control of their work at the workplace. Of course, in these cases, which involve potential infringement on privacy, it is necessary, prior to registration of such processing, to request additional information or commence proceedings pursuant to Article 17 of the Act, which can also result in issuance of a decision on rejection of personal data processing in the notified manner. Protection of property against theft, prevention of vandalism and protection of persons have become the most frequent reason stated for installation of cameras and, simultaneously, the purpose of processing. It appears that fear of theft and vandalism is the most frequent reason for installation of video surveillance systems. However, a controller who intends to install a video surveillance system should always bear in mind the principle of proportionality of the processed data to the declared purpose. In principle, a video surveillance system may be used in cases where the pursued purpose cannot be effectively attained by other means, i.e. where all other options of prevent-

ing unfavorable phenomena at the monitored place have been used. This principle is still not being adequately acknowledged by the controllers and cameras are installed even in places where there is no serious reason for their use. Installation of cameras in schools (in cloakrooms, in corridors, at the entrance) for the reason of protection against theft, prevention of vandalism and bullying is very "popular" and common. Of course, the above considerations again apply in this case. Furthermore, it is necessary that the school inform its pupils and students and their parents of its intention pursuant to Article 11 (1) and (2) of the Personal Data Protection Act in advance and, unless it demonstrates a qualified reason that would authorize it to process personal data without the consent of the data subject, it is necessary that the school obtain the consent of the students to processing of their personal data. In case of minors, this consent must be provided by their statutory representative.

Given the certain specificities of processing of personal data through video surveillance systems, a supplementary form has been created for notification of personal data processing in such systems. This supplementary form is part of the registration form and is available to the controllers on the Office's website.



Transfer of Personal Data Abroad

The conditions and circumstances, under which personal data may be transferred abroad, are stipulated in Article 27 of the Act. In cases where the contemplated transfer is subject to paragraph 1 or 2 of the cited Article, the Office does not have competence to make a decision on the transfer. In other cases, it is necessary to apply to the Office for authorization prior to the actual transfer.

On the basis of a received application, the Office shall review all the circumstances related to the intended transfer, particularly the source, final destination and categories of personal data that are to be transferred, the purpose and period of processing. A transfer of personal data under Article 27 (3) requires that one of the conditions stipulated by law be fulfilled. The condition set forth under subparagraph a) of the above-cited provision, i.e. that the data transfer is carried out with the consent of, or on the basis of an instruction by the data subject, was employed most frequently in the past period.

Within assessment of several applications, the Office ascertained that the applicants intended to transfer to the U.S.A., in addition to other data, also data on birth numbers of their employees. They usually stated that they required the birth number for identification of the employees within a multinational computer network. However, based on intervention by the Office, which enlightened to the applicants the wider context of the entire subject matter, the applicants waived their intention. Transfer of the birth numbers of the employees must be considered to be absolutely purposeless in this case, as the birth number is a specific institute that is intended exclusively for identification of the data subject within the State administration of the Czech Republic. Treatment with personal data is gov-

erned by a special regime following from Act No. 133/2000 Coll.; however, it also constitutes a personal data in terms of Article 4 (a) of the Act and, therefore, it is always necessary to evaluate, not only legality, but also the purposefulness of treatment with the birth number.

Another interesting case dealt with by the Office in the previous period was concerned with an application for transfer of personal data to all countries throughout the world. The applicant operated an advertising website, where he intended to disclose personal data of the advertisers. When assessing this application, the Office dealt in detail with the issue as to whether this specific case indeed involved transfer of personal data to third countries in terms of Article 25 of Directive 95/46/EC of the European Parliament and the Council. Finally, having considered all the decisive facts, the Office agreed with the conclusions of the European Court of Justice in Luxembourg, as stated in Judgment of the Court of 6 November 2003 in Case C-101/01. It follows from the judgment that there is no transfer of personal data to a third country within the meaning of Article 25 of Directive 95/46/EC where an individual in a Member State loads personal data onto an internet page, which is hosted by a provider established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country. Therefore, the Office came to the conclusion that placement of personal data of a natural person on an advertising website does not involve direct transfer of these data between two specific persons, as displaying of these data by a user in a third country requires that the user find and open the given website. Thus, this is not an act of willful transfer, but rather only publication of the necessary personal data through a website for the purpose of offering sale. Consequently, the Office stated in its decision that loading of personal data onto a website cannot be considered to be a transfer of personal data in terms of Article 27 (4) of Act No. 101/2000 Coll.

Another important case dealt with by the Office in the previous period involved an application lodged by České aerolinie a.s. (the Czech Airlines). The company applied for authorization for a transfer of personal data to the United States within the "APIS System" and within its reservation and check-in systems. The reason for submission of this application lay in the fact that, by its Judgment of 30 May 2006, the European Court of Justice in Luxembourg cancelled the decision of a body of the European Union, on the basis of which the party to the proceedings (together with other European airlines) provided U.S. authorities with personal data of all passengers in the framework of the fight against terrorism. The decision in question was the Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection.

The Court concluded that Commission Decision 2004/535/EC was based on an inapplicable Article of the EC Treaty (Article 95), whereby the matter was covered by the 1st EU pillar, i.e. the area of internal market. Thus, it also rejected the option of assessing the case from the viewpoint of Directive 95/46/EC. According to the Court, the entire matter should have been resolved under the 3rd EU pillar, i.e. in the area of justice and internal security. On these grounds, it annulled the aforementioned Decision and, simultaneously, for the reasons of legal certainty, preserved the effect of the Decision until 30 September 2006. Thereby, it provided a short time period for resolving the newly established situation.

Based on the aforementioned facts, under Article 27 (4) of Act No. 101/2000 Coll., the Czech Airlines applied for authorization to transfer personal data to the U.S. Within its decision making, the Office took into account, inter alia, Article 13 of the Convention on International Civil Aviation (147/1947 Coll.), under

which the carrier must comply with the laws and regulations of a contracting State as to the admission of passengers to or departure thereof from its territory. The Czech Airlines had dealt in a similar manner with the aspect of transfer of personal data to the United States within the APIS system and also within its reservation and check-in systems prior to the date of effect of Commission Decision 2004/535/EC of 14 May 2004. The Office concluded that Article 27 (3) (e) of Act No. 101/2000 Coll. would be applicable to the transfer of personal data within the "APIS System" and, after successful completion of the testing operation, also within the reservation and check-in systems employed by the party to the proceedings, involving a transfer of personal data required for the performance of an agreement involving the data subject and, therefore, accepted the application of the Czech Airlines.

Similar to 2005, applications were mostly lodged in 2006 by responsible entities with respect to a transfer of personal data of employees or clients to parent companies established in the United States of America. In the current globalized world, transfers of personal data within multinational companies have become an everyday need. Therefore, major corporations have been taking steps and adopting binding corporate rules (BCR) in this respect. Article 25 of Directive 95/46/EC of the European Parliament and of the Council laid down the principle that personal data may be transferred to a third country only if the third country in question ensures an adequate level of protection. A transfer of personal data to a third country that does not ensure an adequate level of protection may be carried out only if the controller adduces adequate safeguards with respect to the protection of data. One of the possibilities of ensuring protection and legality of processing and transfers of personal data to third countries lies, in accordance with Article 26 (2) of the Directive and Article 27 (3) (b) of the Act, in adoption of binding corporate rules – BCR. This manner of ensuring legality of transfer of data to third countries on the part of multinational companies is becoming increasingly popular. Especially major multinational companies welcome this option, as BCR are the most straightforward and cheapest way of lawful processing and transfer of data within the entire company. For easier orientation in this issue, the Article 29 Data Protection Working Group (WP 29) has issued several working papers providing guidelines as to the manner of ensuring that BCR can indeed serve as a tool providing adequate safeguards.

In 2006, the Office assessed two applications concerning the BCR that were submitted to it by a foreign supervisory authority for approval. In one of the cases, it stated that the BCR complied with all the criteria required for it being considered a tool ensuring adequate protection of personal data in their processing and transfers to third countries. In the second case, the Office came to the opposite conclusion and noted several necessary modifications.

Another possibility of safeguarding protection and legality of processing and transfer of personal data to third countries consists in the use of standard contractual clauses. The exporter of personal data concludes an agreement on transfer of personal data with the recipient of personal data in a third country, including an integral contractual clause pursuant to the Commission Decision (Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC; Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC; Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries). The exporter of data in the EU and the recipient of data in a third country may choose a specific set of contractual

clauses or opt for some other legal basis for the transfer of the data, e.g. the binding corporate rules – BCR (see above). Where, for instance, the controllers have positive experience with the use of contractual clauses of 2001, they may continue to use them. It is important that the main principles expressed in the clauses be respected. These include particularly the right of the data subject to access the personal data that are processed in relation to him and the right to have inaccurate or incomplete data corrected or deleted, the right of the data subject to use a remedy in case of breach of his right, as well as the right to indemnification from the controller. The data subject must be informed on the purposes of processing and the controller's identity. Personal data must be processed only for expressly specified and legitimate purposes.

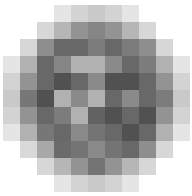
Where standard contractual clauses under the Commission Decision are used for the transfer of personal data, such transfer is not subject to the authorization process in terms of Article 27 of the Act, but rather only to the notification duty pursuant to Article 16 of the Act. Where "non-standard" (ad hoc) clauses are used, the exporter of data is obliged to apply for authorization pursuant to Article 27 of the Act and the Office subsequently verifies as to whether the presented clauses provide adequate safeguards for privacy and the fundamental rights and freedoms of the data subject.

The option of transferring personal data to third countries on the basis of an agreement that includes standard contractual clauses is relatively frequently used by the controllers. This follows from numerous telephone and written inquiries, as well as from the submitted registration notifications.

In some cases, the controllers applied to the Office for authorization of transfer of personal data to countries that are considered to be safe from the viewpoint of personal data protection. This included particularly countries that have ratified Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, ETS 108, 1981) and whose legal regulations thus ensure adequate protection of personal data. Such applications were set aside pursuant to Article 43 (1) of the Code of Administrative Procedure, as neither the Office nor any other administrative authority was competent to make decisions in this respect.

Registration statistics

Total figures as of December 31, 2006		2006	2005	2004	2003	2002
Total number of notifications	28 591	1 450	1 099	1 972	3 187	3 801
Cases of processing registered	26 249	1 195	466	1 591	2 854	4 301
Controllers registered	23 073	945	419	1 402	2 604	3 967
Registrations cancelled	827	92	111	64	52	112
Number of notifications on a change in the processing	1 597	145	134	192	216	40



Foreign Relations and Participation of the Office in International Cooperation

The contents and organization of foreign relations, including participation in international cooperation, is legislatively based particularly on the provisions of Article 29 (1) (g) of the Personal Data Protection Act, according to which the Office ensures fulfillment of requirements following from international treaties binding the Czech Republic.

Another basic provision of the Act consists in Article 29 (1) (i), which obliges the Office to cooperate with similar authorities in other countries, with institutions of the European Union and with bodies of international organizations operating in the area of personal data protection; in addition, in accordance with the law of the European Communities, the Office must meet the notification obligation towards the institutions of EU.

Cooperation with the EU bodies and partners in the EU Member States is a clear priority within relations of the Office with foreign countries. Therefore, activities of the Office in international context are based mainly on the Treaties establishing the European Communities and the European Union and all secondary law, including binding legal acts in the framework of acquis communautaire in the area of personal data protection, and also Convention No. 108 and other legislative rules valid for the 3rd pillar of EU. Two directives of the European Parliament and of the Council and several subsequent decisions of the European Commission have fundamental importance for protection of personal data. The above-cited documents include the basic Directive in this area – Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data – and also Directive 2002/58/EC, concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications); the decisions of the European Commission are mostly related to the adequacy of protection of personal data in some third countries.

The Personal Data Protection Act was brought into full accord with basic Directive 95/46/EC during the year of accession of the Czech Republic to the European Union through amendment No. 439/2004 Coll., although transposition of the provisions of the Directive into national law had already been mostly ensured since the original date of effect of the aforementioned law in 2000, as acknowledged by all evaluation documents of the bodies of the European Commission in the pre-accession period.

The latter Directive (2002/58/EC) was partly implemented by Act No. 480/2004 Coll., on certain services of the information society and on amendment to some acts, through provisions concerning unsolicited commercial communications (marketing spam). The transposition was completed by Act No. 127/2005 Coll., on electronic communications and on amendment to some related acts, which, however, implemented a number of other directives in the area of telecommunications and electronic communications and networks. The overall responsibility in relation to the two acts is borne by the Ministry of Informatics of the Czech Republic, with

which the Office cooperated in the preparation of the relevant provisions aimed at protection of personal data. The same is true for the partial amendment to Act No. 480/2004 Coll. based on criticism by the European Commission; the draft amendment was prepared in late 2005 and early 2006 and was introduced by Act No. 214/2006 Coll. with effect as of August 1, 2006, except for some provisions effective from January 1, 2007.

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

During the previous year, again, the most important working platform for relations and cooperation with both the European Commission and the partner supervisory bodies in other EU countries was the **Data Protection Working Group established under Article 29 of Directive 95/46/EC (WP 29)**. This is a renowned body of the European Commission with an advisory and independent status, whose members include directly the presidents of the independent supervisory authorities of the EU Member States, who also participate in person in a majority of its meetings. A total of 5 meetings of WP 29 took place in 2006. The most important discussed documents and ideas included, e.g. the draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. This document, which had been prepared by the European Commission and extensively discussed and modified in the bodies of the Council, should replace, supplement and specify the incoherent and incomplete legal basis for personal data protection in cooperation of the police and judicial bodies in the EU and, thus, contribute to the transparency of the 3rd pillar. Variances have occurred, not only in the viewpoints of the individual countries, but particularly between the entities engaged in personal data protection, on the one hand, and the governmental bodies of the Member States competent in the area of security and home affairs, on the other hand. Different opinions are also taken by the Office and the Ministry of Interior of the Czech Republic, particularly from the viewpoint of implementation of the prepared EU legal act, where the Office promotes the widest possible application. The topic was also the subject of an entire extraordinary international conference of representatives of national supervisory bodies in the area of personal data protection held in January 2006 in Warsaw with participation of the Office's representatives.

A series of systems intended in the framework of the EU and connected with development of information technologies, such as ALIMENTA (prosecution of persons owing aliments), e-Call (security in road transport), Card Fraud Prevention Database (fight against fraud connected with payment cards), etc. deserve mentioning from amongst numerous other important topics discussed by WP 29. The repeatedly discussed issue of transfer of personal data from the Passenger Names Record in aviation to the U.S. authorities for the needs of the fight against terrorism and serious crime again became topical in relation to cancellation of the original agreement between the EU and the U.S. by the European Court of Justice due to formal legal reasons and negotiations on a new agreement. Extraordinary attention has been dedicated, from roughly mid-2006, to the "SWIFT case". This matter was initiated by a complaint lodged by Privacy International according to which the glob-

al financial service facilitating international money transfers, SWIFT, with its seat in Belgium and operating under the Belgian laws, had been transferring cumulative records of financial transactions to the U.S. authorities within the fight against terrorism.

WP 29 has also a number of working subcommittees, where the Office is represented by its experts. This includes, e.g., the highly active Internet Task Force.

In addition to the WP 29 platform, an opportunity to pursue close relations and ensure joint addressing of issues of the Office with the competent entity for data protection (C-5 Unit) at the Directorate General "Justice, Freedom and Security" of the European Commission is also provided by participation in the meetings of the Committee for Personal Data Protection established by Article 31 of Directive 95/46/EC (Committee 31), with which the European Commission consults all fundamental decisions and measures in the area of personal data protection. Where the adopted measures are not in accordance with the standpoint of the Committee 31, notice of this fact must be provided to the Council, which may then adopt a different decision. Committee 31 was convened only once in 2006 and its agenda was concerned with several aspects of transfer of personal data to "third" countries. Unlike WP 29, this is a political body with prevailing representation of governmental bodies of the individual countries.

The Working Group for Data Protection (G9) of the EU Council is unambiguously a political body. It restarted the activities in the beginning of 2006 after several years of interruption thanks to the Austrian Presidency. 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. The main substantive item on the agenda of the meeting consisted in the above-mentioned draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. Nevertheless, a major part of the discussions to date have been affected by the ambiguities concerning the mandate of this working group and discussions on its future mission.

However, the Office cooperates with the bodies of the EU Council / Coreper also indirectly, within an intersectoral cooperation. Positively evaluated should be particularly the cooperation with the Ministry of Informatics of the Czech Republic in 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. Within the basic documents for discussion, the Ministry of Informatics favorably responded to the comments and instigations of the Office in the interest of ensuring balance of the discussed documents. The position of the Office is sometimes requested also by the Ministry of Interior of the Czech Republic during elaboration of instructions for discussions of bodies of the Council/Coreper with respect to issues affecting protection of data and privacy. However, 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 increasing security while simultaneously respecting the rights of individuals, including the right to privacy and to adequate protection of personal data.

Cooperation with the Ministry of Interior of the Czech Republic within **preparation for accession to the Schengen Convention**, which is anticipated during the next year, has been very intensive and brought remarkably positive effect. The preparedness of the Office for fulfillment of the competence of independent supervision over functioning of the future Schengen Information System was also evaluated during a visit of foreign experts in March 2006 within the overall evaluation

of preparedness of the Czech Republic for accession to the Schengen area. The mission reached very positive conclusions with respect to the preparedness for accession with respect to issues of personal data protection; nevertheless, several recommendations were presented, including the need for express stipulation of the Office's supervisory competence in a law. A minor draft amendment to the Personal Data Protection Act in this sense has already been prepared.

The high degree of preparedness of the Office for accession to the Schengen area was also acknowledged by the fact that its inspector, Mr. Jan Zapletal, was invited to a team of experts of two evaluation missions abroad – in February 2006 in the Slovak Republic and in September of the current year in Baltic countries (Lithuania, Latvia, Estonia).

An extraordinarily active cooperation is being pursued in the framework of the EU 3rd pillar with the **Joint Supervisory Body of Europol ("JSB Europol")**. The Czech Republic contributes to the work of JSB Europol on the basis of the Europol Convention. The Office has sent its representative to this body in accordance with the provisions of the aforementioned Convention and the national legislation of the Czech Republic. The Office's inspector, Mrs. Miroslava Matoušová, acted as the Vice-Chairman of JSB Europol in 2006 and, in accordance with the rules of its activities, she worked as a member of the Appeals Committee, which resolves and discusses complaints of data subjects. She was also the head of an eight-member international team that performed an inspection at the seat of the European Police Office in the Hague in March 2006. As a member of the working group for third countries, she was involved in monitoring of cooperation of the European Police Office encompassing exchange of personal data. In October 2006, the representative of the Czech Republic was again elected as a Vice-Chairman of JSB Europol.

The working group for police established by the Conference of European Data Protection Authorities constituted another important forum within the sphere of the 3rd pillar. The Office is a member of the Conference and, in 2006, it was actively involved in the work of its body established in response to the preparation of international legal regulations providing for personal data processing by bodies and institutions active in the area of law enforcement in the European Union. Within this topic, both the Conference and its working group responded particularly to the individual versions of the aforementioned draft Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The working meetings of the body are connected, from the organizational viewpoint, with other international events, particularly meetings of joint supervisory bodies of the Member States of the European Union for personal data protection.

Joint activities of representatives of the supervisory bodies in the area of data protection from the countries of Central and Eastern Europe and Baltic countries, which were commenced in 2001 on the basis of an initiative of the Czech Office and the Polish Bureau of the Inspector General for the Protection of Personal Data, also continued in 2006. These activities take the form of working meetings and other contacts, including communication through the common website (www.ceecprivacy.org). For example, the meeting held in Varna, Bulgaria from May 25 to 26, 2006 dealt with topics concerned, in the context of personal data protection, with freedom of speech, spontaneous public interest, political and direct marketing, video surveillance systems, dissemination of knowledge on personal data protection, etc.

Specific importance from the viewpoint of development of bilateral relations with the partner supervisory authorities abroad is attached to two projects involving the Office that are financed from the EU funds, one of which was designed to support obtaining foreign experience by the Office, while the other provided for sharing of experience of the Office in favor of a foreign partner.

"Austrian Project"

An eight-month implementation of the project entitled "Assistance to the Office for Personal Data Protection in Exercising Supervision in Personal Data Protection" began in February. This twinning light project was financed by the European Commission in the framework of the "Transition Facility" program. The general objective consisted in deepening and extending knowledge and experience in supervisory activities in the specific areas of data and privacy protection.

Together with the Austrian Ludwig Boltzmann Institut für Menschenrechte (Ludwig Boltzmann Institute for Human Rights) and with professional support from Österreichische Datenschutzkommission (Austrian Data Protection Commission), the Office organized three specialized working meetings that dealt with the following areas, always from the perspective of data and privacy protection: the electronic communications (particularly e-government), the Schengen Information System, the Europol database, the EU customs information system, and the protection of personal data and privacy at workplace. The last event was a workshop for the professional public and was focused on protection of privacy in electronic communications.

Moreover, foreign experts have compiled two professional handbooks. The first deals in detail with personal data protection in electronic communications, while the second is concerned with the protection of privacy at workplace and provides a suitable tool for everyone dealing with this issue. Both publications summarize the findings and experience of the authors, as well as the results of their consultations with the employees of the Office. Thus, the area of interest of these handbooks corresponds to the needs of the Office, which further increases their suitability for practical use.

Project "Support to the Data Protection Commission of Bosnia and Herzegovina"

The twinning project "Support to the Data Protection Commission of Bosnia and Herzegovina" is one of the projects within the CARDS program, i.e. the EU program of support to the Western Balkan countries. The aforementioned project was assigned to the Office by the European Commission on the basis of a tender procedure commenced in late 2004 and completed by ceremonial signing of the relevant contract on November 3, 2005 in Sarajevo.

The twinning project designated by code BA04-IB-OT-01 was designed for the period of 14 months and funded from the budget of the European Union (the total amount of allocated funds equals approx. EUR 500 000). The Office implements this project as the senior partner in cooperation with the Spanish Data Protection Authority. The beneficiary is the Data Protection Commission of Bosnia and Herzegovina.

The purpose of the project is to contribute to the creation of an environment in Bosnia and Herzegovina that would fully reflect the European standards of personal data protection and thus facilitate accession of the beneficiary country to the European Union. The individual project goals and activities are divided to three main components: analysis of the legal environment for processing and protection of personal data, including indication of the necessary legislative measures; preparation for establishment and creation of a new independent body for protection of personal data in Bosnia and Herzegovina; and, finally, increased awareness of both professional and lay public with respect to the aspects of protection of personal data and privacy.

The project was commenced on February 1, 2006, when the Office sent its expert, Mr. Jiří Maštalka, to Bosnia and Herzegovina; Mr. Maštalka has been in charge of the project implementation in Sarajevo. Short-term experts from amongst em-

ployees of the Office and the Spanish Data Protection Authority are also involved in the fulfillment of the individual project tasks. Two external experts from Great Britain and Italy were also involved in one of the training courses.

The fulfillment of the individual tasks had to be based on the actual state of affairs in Bosnia and Herzegovina. It is important in this respect that the country consists of two entities, i.e. the Federation of Bosnia and Herzegovina, which in turn consists of ten Cantons with a relatively high degree of competence, the Republika Srpska and the special District of Brčko. Furthermore, the supranational Office of the High Representative is also active in the country, having relatively great powers with respect to the internal affairs of Bosnia and Herzegovina. This results in considerable lack of transparency of the legal environment.

The first Personal Data Protection Act of the Bosnia and Herzegovina was adopted in 2001; however, it contained major gaps from the viewpoint of the European legal standards. A new law was therefore drawn up short afterwards; however, following several years of discussion, it was formally adopted only in early 2006. This occurred shortly after commencement of the project; nevertheless it was not possible to intervene in the preparation of the new Act in the framework of the project. The Act contemplates that a new personal data protection authority should be established during the year 2007, replacing the current "Data Protection Commission of Bosnia and Herzegovina" which is operating in absolutely unsuitable conditions.

The following can be stated with respect to fulfillment of the individual project tasks:

1. The legislative area included particularly an overall analysis of the legislation of Bosnia and Herzegovina. Successful fulfillment of this task was facilitated by the fact that the expert sent by the Office for Personal Data Protection was able to communicate in local languages (Bosnian, Serbian and Croatian). The analysis included particularly overall evaluation of the ability of the local legislation to reflect the aspects of personal data protection, conformity of the new Personal Data Protection Act with the European standards, the issue of personal data protection in the police sector and the aspects of personal data protection in some key sectors (health care, banking, etc.).

   This resulted in preparation of first versions of summary materials that will be discussed in January 2007.

2. The preparation of a new independent data protection authority (Agency for Personal Data Protection in Bosnia and Herzegovina) encompassed particularly elaboration of a draft material containing the basic organizational structure of the institution in accordance with the legislation of Bosnia and Herzegovina enabling it to fulfill its tasks in accordance with the European standards. Furthermore, guidelines were drawn up with respect to its key functions, particularly supervisory and registration activities, acceptance of complaints, transfer of data abroad, etc. A number of internal workshops, working meetings and study visits also took place, with the aim of training the competent persons. It should also be noted in this relation that the expert of the Office provided operative assistance in resolving specific matters related to the issue of personal data protection in Bosnia and Herzegovina.

3. An awareness raising campaign has also been part of the project. Its objective is to raise general awareness of protection of data and privacy. An article concerning personal data protection was drawn up in this relation and published in local professional journals. Furthermore, the experts of the Office prepared a guideline concerning the aspects of public relations and a draft promotional leaflet which has

been prepared for printing. It should be distributed at the end of the project. Finally, a note should be made of a number of public workshops concerning specific aspects of personal data protection.

Although the project has not yet been completed, it can be stated that its program was successfully developed during the year 2006. Preconditions have been created for proper performance of all planned activities within the set deadline, i.e. by March 31, 2007, when the project is scheduled to end. The positive response is also documented by the fact that the expert of the Office sent to Bosnia and Herzegovina discharged, on the basis of request of the local authorities, the office of observer of the OSCE (Organization for Security and Cooperation in Europe) within the local general elections held on October 1, 2006. It should be added that, outside the framework of official participation in the projects, the Office also held in Prague a workshop for the Personal Data Protection Commission of Macedonia, where the foreign colleagues were provided with valuable information and a number of recommendations suitable for development of their new supervisory activities.

The continuing participation of the Office in activities following from the obligations of the Czech Republic as a member state of the **Council of Europe** and OECD is also noteworthy in relation to fulfillment of the requirements of the international agreements. 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), which is the supreme body of the Council of Europe dealing with data protection. Under its coordination, the Council of Europe declared a Data Protection Day in 2007, which will commemorate the fact that Convention No. 108 was opened for signatures on January 28, 1981. The Czech Office is also greatly involved in this project, which is aimed at raising public awareness of personal data protection.

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

In addition to the aforementioned activities in the framework of regular cooperation within the above-listed working bodies of international organizations and bilateral cooperation with the partner authorities, the experts of the Office participated in a number of ad hoc and regular events, such as conferences, workshops and meetings of various types. These include, in particular, the following important events:

"Conference of European Data Protection Authorities"
(Belgium, Brussels, January 24, 2006)

An extraordinary conference of the European data protection authorities was concerned with the preparation of an opinion on two draft legislative acts of the European Union with respect to processing of personal data by law enforcement bodies, i.e. the Draft Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters and the Draft Framework Decision on exchange of information under the principle of availability.

"Legal Framework for the Information Society"
(Italy, Florence, February 10 – 11, 2006)

The program was concerned with exchange of experience in the area of legal aspects of information and telecommunication systems, personal data protection and teaching of computer law in the EU countries.

"Meeting of the Task Force Spam; OECD/ICCP Workshop on the Future of the Internet" (France, Paris, March 6 – 8, 2006)

The meeting of the Task Force on Spam was concerned with completion of the "Antispam Toolkit", which consists of several recommended subjects in the area of the fight against spam, e.g. from the viewpoint of legislative approaches, initiatives of the industry, technical designs, education and awareness, global cooperation, measurement of spam and effective enforcement of the valid rules.

"13th Case Handling Workshop" and "14th Case Handling Workshop" (Spain, Madrid, March 26 – 29, 2006 and Greece, Athens, November 13 – 14, 2006)

The major topics of the 13th Case Handling Workshop included the subject of personal data protection in electronic communication of governmental bodies (e-government). In addition to e-government, the 14th Case Handling Workshop dealt particularly with the subject of video surveillance, implementation of Directive 2002/58/EC, finance and banking sector.

"1st European Congress on Data Protection"
(Spain, Madrid, March 27 – 31, 2006)

The individual items on the agenda of the Congress concentrated on the contemporary important challenges in data protection – protection of personal data particularly in relation to security, market, freedom of speech, transparency and access to information.

"Annual Spring Conference of the European Data Protection Commissioners" (Hungary, Budapest, April 24 – 25, 2006)

The senior representatives of personal data protection supervisory bodies again met at their annual conference. They discussed topical issues, such as localization through GPS (geolocalization), medical documentation in a joint register, disclosure of files of the former State security corps, genetic data, etc. A joint declaration was adopted with respect to the search for balance between increased powers of the police and courts as a consequence of the fight against terrorism, on the one hand, and freedom of citizens, on the other hand.

"Conference on Public Security and Data Protection"
(Poland, Warsaw, May 11 – 12, 2006)

The conference which involved important representatives of national and international bodies in the area of personal data protection, was concerned with person-

al data protection particularly within the EU 3rd pillar. This event was organized by Mrs. Ewa Kulesza at the occasion of her resignation from the office of Inspector General for the Protection of Personal Data in Poland.

"8th meeting of Contact Network of Spam Authorities (CNSA)"
(Belgium, Brussels, June 7, 2006)

The 8th meeting of representatives of the national law enforcement bodies in the area of unsolicited commercial communications sent through the Internet and other electronic means was dedicated primarily to strengthening of international cooperation of the participating bodies and creation of standardized mechanisms for dealing with this issue.

"Workshop of the European Contact Network of Anti-Spam Authorities (CNSA)" and the "4th German Anti Spam Summit"
(Germany, Cologne, September 4 – 5, 2006)

The "SpotSpam Workshop" was organized as a working meeting of the representatives of supervisory bodies associated in the CNSA for the purpose of presenting one of the last versions of the SpotSpam project – a knowledge database serving for storage and exchange of information required for the performance of effective inspections and administrative proceedings against disseminators of unsolicited commercial communications.

"Workshop on Data Protection Problems in E-Government and RFID technology"
(Austria, Vienna, October 5 – 6, 2006)

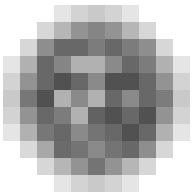
This workshop was concerned with the aspects of identification, pseudoanonymization and application of RFID radio-frequency technologies. The aspects of identification, particularly with the use of RFID, are a topical issue with a great potential in the near future.

"28th International Conference of Data Protection and Privacy Commissioners"
(United Kingdom, London, November 1 – 3, 2006)

58 agencies for protection of data and privacy from various countries participated in this event. It also involved a wide range of governmental, judicial, civic and social, as well as private organizations. A majority of the conference was dedicated to assessment of phenomena in a monitored society and their impact on the life of an individual.

"Visit to the Romanian Personal Data Protection Authority"
(Romania, Bucharest, February 13 – 14, 2006)

This was the first official visit of the President and the spokeswoman of the Czech Office to the Romanian National Supervisory Authority for Personal Data Processing, shortly before accession of Romania to the EU. The objective was to share the experience of the Office – particularly with preparation of annual reports – and establishment of closer contacts. The agenda of the visit to Bucharest was based on the working meeting with several experts of the Romanian Authority in Prague in May 2006 and with the President of the Romanian Authority in Varna.



The Office, Media and Means of Communication

In 2006, the Office continued to apply methods of communication that had proved effective over the recent years and that create a picture of an institution that consistently fulfills the duties imposed on it by the law: particularly, the tradition of regular quarterly press conferences was maintained; these conferences describe the quarterly work of the Office and, at the same time, summarize the cases that appeared as the most important for personal data protection from the viewpoint of control activities, as well as cases that were opened with contribution of the media and specific journalists. This includes raising of awareness amongst the general public with respect to aspects of personal data protection in line with the concerns of the citizens related to the protection of privacy and, in relation to the media, it also fulfills the consultation duty that is generally imposed on the Office by law.

With respect to the year 2006, similar to the previous year, it can be stated that the questions presented to the Office by journalists reflected their great trust in credibility and expertise of this institution. The journalists again put forth questions exceeding the scope of competence of the Office and, nevertheless, they were absolutely sure that they would get, if not direct answers, then at least basic advice and information as to where they could obtain detailed description.

There were practically no more cases of journalists eagerly expecting that the legal problem could be resolved by an immediate statement as to whether or not the law had been violated. Let us hope that this fact documents gradual improvement of legal awareness. The Office has also not encountered any simplification of its explanations or their serious manipulation. Misinterpretation, which was probably caused by an effort to provide an up-to-date report, rather than due to deeper adverse motivation, was a rare phenomenon.

The regular press conferences have resulted in a repeated increase in the number of news articles, sometimes very extensive (e.g. up to 70 articles in three days following after the conference). However, it can be generally stated, e.g. based on statistical data, that the number of media reports exceeds the number of working days in a year (cf. the table on p. 68).

Special activities pursued during the year included cooperation with the Data Protection Commission of Bosnia and Herzegovina, for which the employees of the Press Department organized workshops in Sarajevo and Prague and drew up a guideline of principles of communication and cooperation with the media, both in the framework of the Office's twinning program (for more details, see the chapter entitled Foreign Relations and Participation of the Office in International Cooperation). This program will continue next year.

The Office also shared its experience with Romanian and Macedonian colleagues who contributed to establishment of supervisory authorities for personal data protection in their respective countries.

PRESS CONFERENCES

The press conference held in January was exceptional to a certain degree. It commemorated the 25th anniversary of opening Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data for signatures and the Data Protection Day prepared by the Council of Europe. It also commemorated, as an important historical date, the Holocaust Memorial Day which was promulgated in 2005 by the UN. Indeed, it is a sad fact that unprotected sensitive data on nationality played an important role in the tragedy of the Jewish population.

A press conference was held at the end of November in the presence and with assistance of Austrian partners, with whom the Office cooperated for a period of six months within a twinning project (for more details, cf. Foreign Relations and Participation of the Office in International Cooperation). This conference was also broadcast in two parts on the 24.CZ TV station.

Almost every press conference, as well as the issues dealt with at the conference, is promoted within morning broadcasting of the Czech Television and TV NOVA, where the President of the Office is usually invited as a guest, and the morning broadcasting of CRo1 Radiožurnál (Czech Radio).

In addition to the current report by the President of the Office, facts related to the work of the individual units of the Office, statistical surveys of commented drafts of acts and other legislation and surveys of fines imposed by the Office during the given period were, as usual, provided at the press conferences; the journalists were also informed of the most important documents through which the Office expressed its standpoints during the relevant quarter in relation to the subject of personal data protection. A survey of the state of investigation in cases that are pursued or detected, or submitted to the Office by the media, usually receive, for absolutely comprehensible reasons, the greatest interest of journalists.

An important part of every press conference is dedicated to a certain segment of work of the Office: for example, at the press conference held in September, the Office presented a new registration process which, due to commencement of electronic submission of registration forms, provided the potential personal data controllers with greater user comfort thanks to the possible internet communication and the detailed and user friendly form.

PUBLISHING ACTIVITY – DISSEMINATION OF NEW EUROPEAN AND GLOBAL FINDINGS

In 2006, the Office issued four editions of the Journal. The number of editions was the same as in the previous year.

The positions issued by the Office, surveys of general aspects of its decision-making activities, and translations of pan-European documents concerning personal data protection – which are often directly adopted from the Official Journal of EU – are then published on the Office's website. The Office considers these communication links to be beneficial, as they extend the number of recipients of the relevant information.

The Information Bulletin of the Office is a quarterly publication intended for a wider public, unlike the Journal, which is aimed at the professional public. The fact that 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, apparently bears its fruits: the interest shown in this periodical by various institutions documents its increasing referential character. Of course, this is welcomed by the Office; however, it obliges it for the future.

An absolutely special position amongst the periodicals issued by the Office was occupied by Information Bulletin No. 2 of 2006. This entire volume was dedicated to children and the aspects of protection of children's personal data; however, it was also intended for the parents. On the basis of negotiations with the Ministry of Education, Youth and Sports, this volume of the Bulletin was offered for use in teaching. The Office noted with satisfaction the high interest and favorable responses from schools; even though distribution and additional printing of this volume – in accordance with the requirements of the schools – increase the workload, the Office has decided to satisfy all the requirements (the Office is both the author and editor of the Information Bulletin and it is also printed and distributed by it). Simultaneously, this volume of the Bulletin raised considerable interest on the part of foreign partner authorities, which increasingly feel the need for effective communication with the citizens. Therefore, the Office has decided to translate this volume into English and provide it to its foreign partners. However, it will play a particularly important role within the prepared information campaign aimed at older children of school age (cf. the subchapter Other Communication Procedures below).

The publishing activities of the Office were subject to control performed by the Supreme Audit Office, which has not found any inadequacies on the part of the Office; on the contrary, the issue of a leaflet by the Office in 2004 constituted a criterion of the lowest costs.

OTHER MEANS OF COMMUNICATION

The website of the Office underwent substantial restructuring at the end of 2005; these changes were aimed at ensuring greater awareness of the general public. The increased comfort of potential personal data controllers, who can employ the newly conceived form which may be submitted electronically, was already mentioned above. A concept of a special section dedicated to the aspects of personal data protection within the Schengen Information System was drawn up at the end of the year. This project was based on the preparation of an information campaign for citizens, whose coordination was entrusted by the Government of the Czech Republic to the Ministry of Interior and in which the Office for Personal Data Protection is involved.

In 2006, the Office implemented an extensive information project for the citizens: in cooperation with BENY TV, it prepared 13 parts of series "Ignorance does not excuse, or Everyone has secrets". The series were concerned with the basic aspects of the Personal Data Protection Act and explained the Act and the principles of protecting privacy in a very illustrative manner acceptable for a wide range of spectators. The series were broadcast over a period of 13 weeks by the Czech Television and its first-time broadcast parts were watched by 160 000 to 310 000 viewers (in addition, the series were twice repeated). Next year, the series will be placed on the Office's website and a copy will be provided to the parties interested in its non-commercial use (i.e. educational institutions, local governments, non-governmental organizations, etc.). The Office will provide a DVD with the series also to teachers participating in the prepared workshops in 2007 (cf. below).

In January 2007, the Office will participate in the project initiated by the Council of Europe, the "Data Protection Day" (January 28). For this occasion, the Office's Press Department has prepared a competition for children called "My privacy! Don't look, don't poke about!". The competition will be announced at the press conference held in January and, for a period of four months, will be promoted by CRo2 Praha (Czech Radio 2), the Ministry of Education, Youth and Sports and the International Film Festival for Children and Youth. Previously issued Information

Bulletin No. 2/2006 and the aforementioned television series will be used for this competition. In early December, the project of the Czech Office made a great impression on the expert group of personal data protectors of the Council of Europe, which requested that it be presented at the plenary meeting as an inspiration project.

An idea of creating a program for DVPP (ongoing education of pedagogic workers) arose in the context of negotiations with the Ministry of Education, Youth and Sports on the aforementioned project. The Press Department of the Office has prepared the project and presented it for accreditation. This was the first step aimed at making personal data protection, as a legal tool for protection of privacy, one of the fundamental values of our civilization, part of the educational process in the Czech Republic. The project obtained accreditation of the Ministry on December 15, 2006. As every year, the lawyers of the Office provided lectures within their contractual obligations. The Press Department provided a special workshop for the students of the 3rd Faculty of Medicine of Charles University within a lecture on doctor's ethics.

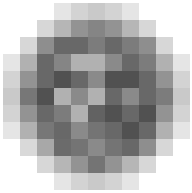
Within its competence and the related limitations, the Office has cooperated with the Iuridicum Remedium civic association, which also deals with personal data protection. The President of the Office made an important presentation at a conference organized by the association in August 2006 on the subject of protection of personal data in traveling. The Office also provided professional advice related to the education film concerned with personal data protection, which was prepared by Iuridicum Remedium last year.

LIBRARY AS A PROFESSIONAL BACKGROUND

The 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 regular supplementation of books and periodicals (in 2006, the library was supplemented by 130 books, of which 81 were obtained by purchase and 49 as a gift), at the end of the year, the library expanded its collection by a survey of foreign publications in periodicals containing important articles on the current topics of personal data protection that became the subject of expert specialization of inspectors and professional employees of the Office in 2006. The articles are collected on the basis of surveys carried out by the Press Department and are also available in electronic form on the Office's website.

COMMUNICATION OF THE OFFICE WITH MEDIA IN FIGURES:

Agency service	31
Total press	184
of which:	
Daily press	90
Other periodicals	94
Television	59
Radio	31
Total media	**305**



Information Provided Pursuant to Act No. 106/1999 Coll., on Free Access to Information

Re: Article 18 (1) (a)

In 2006, the Office received 9 inquiries qualified by the inquiring parties as request for information pursuant to Act No. 106/1999 Coll. as amended.

However, all inquiries were dealt with by reference or advice of their correct qualification.

Re: Article 18 (1) (b)

During 2006, the Office received 4 inquiries pursuant to the Act on Free Access to Information.

Two other cases related to a duty following from Act No. 101/2000 Coll., as amended, and, in two cases, the inquiring party requested explanation of the relation between the Personal Data Protection Act and the Act on Free Access to Information; one inquiry was concerned with the duties following from Act No. 101/2000 Coll., on personal data protection, and Act No. 500/2004 Coll., the Code of Administrative Procedure.

Re: Article 18 (1) (c)

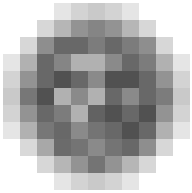
Not applicable in 2006.

Re: Article 18 (1) (d)

No proceedings on penalties were held

Re: Article 18 (1) (e)

Not applicable in 2006.



IT in 2006

Renewal and development of the information system took place in 2006 with respect to several basic aspects:

1. Continued renewal of hardware
2. Replacement of the basic SW in offices
3. Upgrade of the filing service together with a new module supporting administrative proceedings
4. New option for lodging notifications of processing of personal data
5. Creation of the role of a security manager
6. Preparation of a SW module supporting purchase of assets and services
7. Creation of a centrally managed

The renewal of hardware continued by replacement of obsolete workstations so that a uniform working environment could be used in all computers of the Office based on the license agreement with Microsoft. Thus, the employees of the Office currently use a uniform working environment on their personal computers that have an adequately fast response and storage capacity. The computers are also prepared for a potential change in the environment brought by a new operational system and office applications in relation to the newly prepared Microsoft products.

A tender procedure was held in connection with the requirement for SW supporting administrative proceedings; the product of the Gordic company was selected. As this product is relatively firmly linked with the GINIS filing service, this decision also included a transfer of the filing service to GINIS. Both the filing service and support for administrative proceedings were put into operation on January 1, 2007.

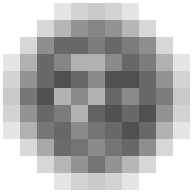
Amendment to Act No. 101/2000 Coll., on personal data protection, required modification of the registration methodology and a change in the form for notifying personal data processing. The paper version of the optically processed registration form was cancelled and a new version of the form was prepared, which is available on the Office's website and allows for lodging notifications of personal data protection by electronic means. The browsing system of the Public Register of Personal Data Processing was also modified, allowing for search for registered controllers on the Office's website.

The IT Department continued to improve the security of the Office's information system. A security audit was carried out during the year in cooperation with a specialized company, including external and internal penetration tests, creation of a User Security Guidebook and preparation of a Guideline for ICT/IS Security Management. This created a basis for establishment of the position of security manager. Great attention continues to be paid to antivirus and antispam protection. The number of spam messages in e-mail communications of the Office increased approximately eight times compared to the previous year.

The project support process related to acquisition of property and services based on the applicable legislation was initiated in 2006. The prepared product will support and document all processes required pursuant to the applicable legislation upon purchase of property and services. It will use electronic signature and support electronic filing so that the relevant documents need not be filed in paper form. The system will be linked with other modules of the information system and will maximally support the users and provide them with all relevant information that may be provided at the time of decision-making by other sources within the Office's IS. Pilot operation of the module will be commenced in the 1st quarter of 2007.

The projects implemented last year included the project of documentation of the building. This application of the graphic information system covers, not only the building, but also a number of other internal relations and entities and a link to its parts is also provided for other modules of IS. The module is currently in testing operation.

The central system of printing and copying services was also put into operation last year. The system utilizes as much as possible, multifunctional equipment and network printers. It also allows for automatic monitoring of printing and copying costs of the individual departments. The reason for introducing this system lay in the efforts to reduce the costs of printing and copying.



Personnel of the Office

As of December 31, 2005, the Office for Personal Data Protection had 80 employees (a period of notice of termination was pending in relation to 4 of these employees); the State budget for 2006 set the planned number of employees at 90.

Recruitment of new employees was driven by the effort to create a functioning service for the inspectors of the Office and, therefore, it was aimed particularly at providing high-quality personnel for the newly established working positions within the Inspectorate. As high professional demands are placed on majority of employees of the Office and language skills are also required from selected employees, specialized workshops and language courses were again organized in 2006 for employees according to their job tasks.

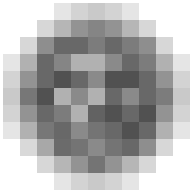
As of December 31, 2006, the Office had 89 employees.

Classification of employees of OPDP according to age and sex – as of December 31, 2006

Age	men	women	total	%
21 to 30 years	6	12	18	20,2%
31 to 40 years	6	4	10	11,2%
41 to 50 years	7	11	18	20,2%
51 to 60 years	23	14	37	41,6%
61 and older	5	1	6	6,7%
Total	47	42	89	100%
%	52,81%	47,19%	100%	

Classification of employees of OPDP according to education and sex – as of December 31, 2006

Education	men	women	total	%
Basic	0	0	0	0,0%
Vocational training	2	0	2	2,2%
Secondary vocational	0	1	1	1,1%
Full secondary	3	6	9	10,1%
Full secondary vocational	5	16	21	23,6%
Higher vocational	0	2	2	2,2%
Bachelor's	1	0	1	1,1%
University	36	17	53	59,6%
Total	47	42	89	100%



Economic Management of the Office

The budget of the Office was approved by Act No. 543/2005 Coll., on the state budget of the Czech Republic for 2006.

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

Summary indicators	in CZK thousand
Total non-tax and capital income and accepted subsidies	3 995,32
Total expenditures	83 788,04

Cross-cutting expenditure indicators

Salaries of employees and other payments for performed work	35 882,82
of which: salaries of employees	34 374,34
other payments for performed work	1 508,48
Mandatory insurance premiums paid by the employer *)	12 463,22
Contribution to the Cultural and Social Needs Fund	687,49

*) premiums for social security and the contribution for the state employment policy and premiums for public health insurance

Individual indicators:

Expenditures for financing programs pursuant to Schedule No. 5	21 170,82
of which: capital expenditures	7 151,67
non-investment expenditures monitored in ISPROFIN	14 019,15
Common non-investment expenditures and related expenditures	13 583,69
Transfer to the reserve fund	2 877,49

Specific indicators – income

Total non-tax and capital income and accepted subsidies	3 995,32
of which: total income from the budget of the European Union	2 146,00
of which: Twinning Out project – Bosnia and Herzegovina	2 146,00

Specific indicators – expenditures

Expenditures for the performance of tasks of the OPDP	83 788,04
of which: salaries of employed officers derived from salaries of constitutional officials	8 398,39
reimbursement of expenditures related to the discharge of the office (Act No. 236/1995 Coll.)	1 917,07
expenditures for financing the EU Twinning Out project – Bosnia and Herzegovina	2 161,61
expenditures for financing the EU Twinning Light project – Austria	16,04

Income

The budgeted income for 2006 equaled CZK 3 632 thousand. The total income of Chapter 343 – Office for Personal Data Protection equaled CZK 3,995.32 thous.

This income consisted particularly of refunds for foreign trips of employees of the Office from the Council of Europe and the European Commission, penalties imposed pursuant to Act No. 480/2004 Coll., on certain services of the information society, reimbursement of the costs of the proceedings, interest on money deposited in accounts kept by the Czech National Bank, an insurance benefit, transfers from own funds and income related to 2005 (transfer of the balance of the deposit account after payment of salaries and the allocation to the Cultural and Social Needs Fund for December 2005) and, particularly, refund of money drawn from the Twinning Out project – Data Protection Commission of Bosnia and Herzegovina in the amount of CZK 2,146.00 thousand.

The income account included the use of money from the reserve fund in a total amount of CZK 1,407.11 thousand, for the supplementation of the mobile equipment on the premises of the Office.

Interest on money deposited in accounts kept by the Czech National Bank equaled CZK 3.65 thousand.

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

1. Common expenditures

Withdrawals for common expenditures in an amount of CZK 27,602.84 thousand correspond to the common operational expenditures that follow from the main activities of the Office, including particularly items connected with purchase of minor tangible assets, materials, services, travel allowances, maintenance and expenditures related to non-investment purchases. Expenditures for supplies of water, gas and electricity equaled CZK 900.75 thousand in 2006. The aforementioned amounts correspond to the requirement for purposeful and economic operation of the Office.

2. Salaries of employees and other payments for performed work

Withdrawal of the budget for salaries of employees and other expenditures for the performed work correspond to the qualification structure and fulfillment of the plan by the employees. As of December 31, 2006, the personnel consisted of 89 employees.

3. Expenditures for financing programs included in the information system of the Ministry of Finance – ISPROFIN

A total of CZK 21,170.82 thousand was withdrawn in accordance with the approved documentation of program 243 010 "Development and renewal of the material and technical background for the Office for Personal Data Protection". Of this amount CZK 7,151.67 thousand were drawn for investment expenditures (of which CZK 432.51 were transferred to the reserve fund). These expenditures included particularly the following expenditures in program 243010 "Development and renewal of the material and technical background":

subprogram 243 011 "Acquisition, renewal and operation ICT OPDP",
where investment expenditures from the state budget
were incurred in 2006 for

	in CZK thous.
project 243011 0006 "Acquisition and renewal of computers"	133.72
project 243011 0014 "Upgrade of Microsoft servers and the OS of workstations"	2 582.52

project 243011 0015 “Development of the OPDP IS – module Register”	1 204.14
project 243011 0016 “Acquisition or property and services”	900.83
project 243011 0018 “Development of the OPDP IS – upgrade of module NOS”	237.27
project 243011 0019 “Records of attendance of employees”	87.66
project 243011 0020 “Upgrade of the Intranet application”	0.00
project 243011 0025 “Documentation of the building”	297.66
project 243011 0027 “Upgrade of the filing service system including the module for admin. proceedings”	1 119.65

systemic non-investment expenditures from the state budget for:

project 243011 0006 “Acquisition and renewal of computers”	1 596.17
project 243011 0022 “Extension and renewal of licenses of the AVG antivirus program”	57.60
project 243011 0024 “Employee certificates”	69.55
project 243011 0026 “Management of IS security”	407.34
project 243011 0027 “Upgrade of the filing service system including the module for admin. proceedings”	91.50
project 243011 0031 “Introduction of bar codes”	81.64
project 24301P200 “Operation of ICT of the Office”	6 046.91

subprogram 243 012 “Reproduction of the OPDP assets”
where investment expenditures from the state budget were incurred for

project 243012 0120 “TV reception"	44.71
project 243012 0121 “Reconstruction of kitchenette and WC”	111.00

systemic non-investment expenditures from the state budget for:

project 243012 5501 “Rent and services”	2 947.30
project 243012 5502 “Maintenance of equipment and long-term investment assets”	1 194.03
project 243012 5503 “Provision of mobile equipment for offices”	1 407.11

(means for this fund were withdrawn from the reserve fund)

Non-investment systemic expenditures were withdrawn in an amount of CZK 14,019.15 thousand (of which CZK 120 thous. were transferred to the reserve fund) and were used for payment of ICT operational costs, services and maintenance of equipment and minor long-term tangible assets.

4. Internal audit and internal control

The internal audit was staffed only in the 2nd half of 2006 and, in accordance with the adopted plan, an external audit was carried out by Český a moravský účetní dvůr, s.r.o., aimed at conformity of the internal regulations of the OPDP with the applicable legislation of the Czech Republic and the European Union. The findings are gradually incorporated in the internal guidelines.

5. Use of the reserve fund

Part of the means in the reserve fund were used to finance subprogram 243012 5503 “Provision of mobile equipment for offices”, in an amount of CZK 1,407.11 thousand.

Survey of use of the budget in 2006

Budgetary item	Name of indicator	Approved budget for 2006 in thous. CZK	Modified budget for 2006 in thous. CZK	Actual facts pursuant to the accounting records as of 31-Dec-06 in thous. CZK	Fact /modif. budget in %
	TOTAL INCOME	**0**	**0**	**41 052,29**	**0**
501	Salaries	34 434	34 974	34 374	98,28
5011	Salaries of employees	20 111	20 111,00	20 104,09	99,97
5014	Salaries of employees derived from salaries of constitutional officials	7 955	8 404	8 398	99,93
502	Other payments for performed work	2 121	2 121	1 508	71,10
5021	Other personnel expenditure	1 821	1 821	1 420	77,98
5024	Severance Pay	300	300	88	29,49
5026	Severance pay	0,00	0,00	0,00	0,00
503	Mandatory insurance premiums paid by the employer	12 795	12 984	12 463	95,99
5031	Mandatory premiums for social security	9 505	9 645	9 270	96,11
5032	Mandatory premiums for public health insurance	3 290	3 339	3 193	95,64
513	Purchase of materials	8 570	6 450	4 739	73,47
514	Interest and other financial expenditure	100	100	16	16,36
515	Purchase of water, fuels and energy	1 770	1 810	1 250	69,05
516	Purchase of services	13 728	17 148	13 415	78,23
5167	Training and education	1 000	1 000	849	84,89
517	Other purchases	9 834	9 390	3 774	40,19
5171	Repairs and maintenance	5 000	4 450	748	16,81
5173	Travel allowances	2 500	3 600	2 502	69,51
518	Advance payments provided	0	0	0	0
519	Expenditures related with non-investment purchases	2 290	2 290	1 952	85,23
5342	Transfers to the Social and Cultural Needs Funds	689	700	688	98,21
5346	Non-investment transfers to the RF			2 445	
536	Other non-investment transfers to public budgets	11	15	12	85,53
542	Compensation to citizens	60	60	0	0
5429	Other compensation to citizens	60	60	0	0
	TOTAL CURRENT EXPENDITURES	86 402	88 042	76 636	87,04

Budgetary item	Name of indicator	Approved budget for 2006 in thous. CZK	Modified budget for 2006 in thous. CZK	Actual facts pursuant to the accounting records as of 31-Dec-06 in thous. CZK	Fact /modif. budget in %
611	Acquisition of long-term intangible assets	398	6 710	6 271	93,45
612	Acquisition of long-term tangible assets	8 622	670	448	66,93
6361	Investment transfers to the RF			433	
	TOTAL CAPITAL EXPENDITURES	9 020	7 380	7 152	96,91
	TOTAL EXPENDITURES	**95 422**	**95 422**	**83 788**	**87,81**
	of which: use of the reserve fund			1 407	

ANNUAL REPORT 2006

THE OFFICE FOR PERSONAL DATA PROTECTION

PPLK SOCHORA 27, 170 00 PRAHA 7

E-MAIL: INFO@UOOU.CZ, WEB: WWW.UOOU.CZ

IN FEBRUARY 2006, THE ANNUAL REPORT WAS PUBLISHED ON THE BASIS OF DUTY IMPOSED BY ACT NO. 101/2000 COLL., ON THE PROTECTION OF PERSONAL DATA AND ON AMENDMENTS TO SOME RELATED ACTS, ARTICLES 29 (D) AND 36.

EDITOR: HANA ŠTĚPÁNKOVÁ, TEL. + 420 234 665 286; FAX + 420 234 665 505

EDITORIAL STAFF: JAN FOLDA, ANDREA SKLENÁŘOVÁ

GRAPHIC LAYOUT: MILOSLAV ŽÁČEK