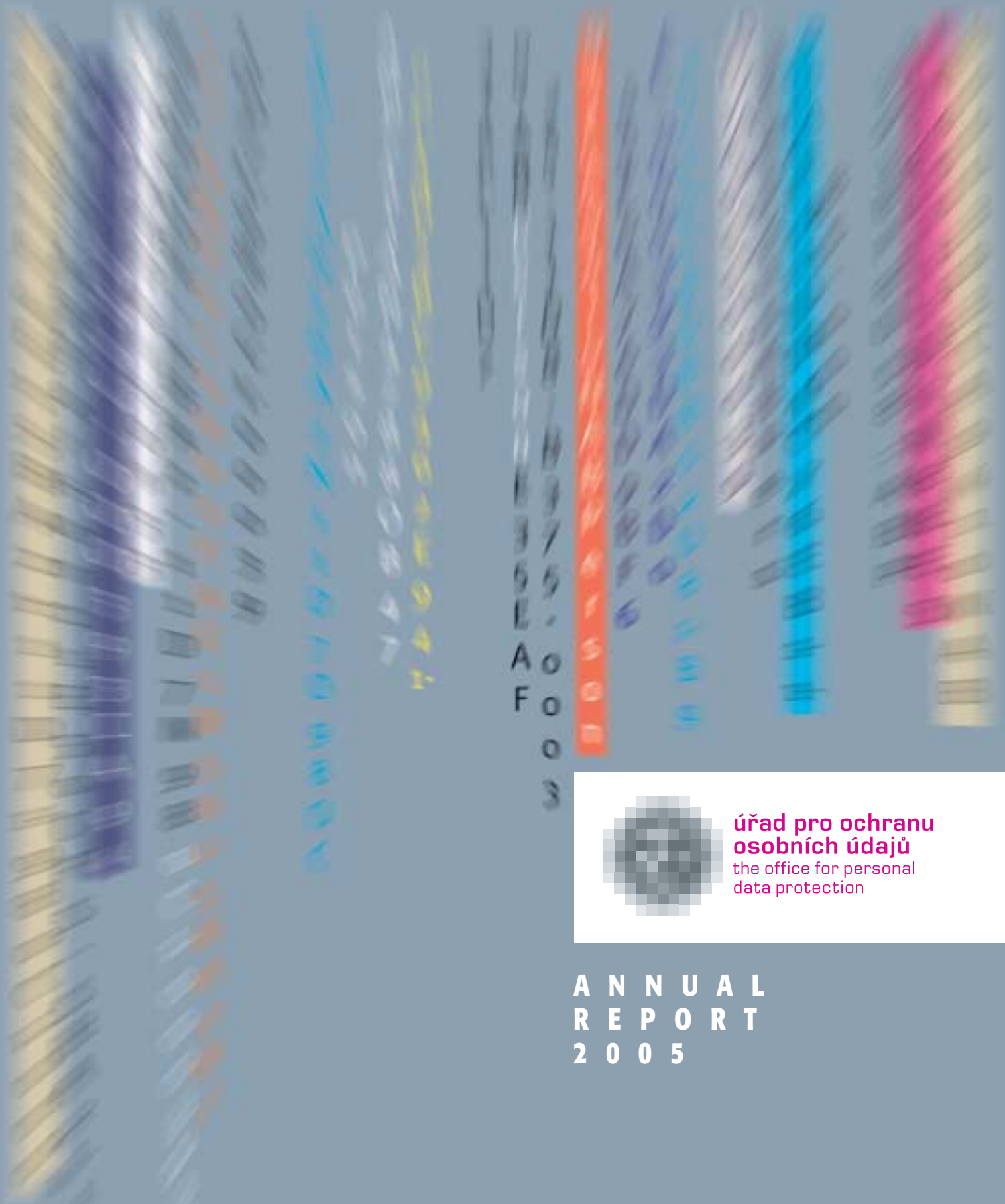


úřad pro ochranu osobních údajů
the office for personal data protection

ANNUAL REPORT 2005

Contemplation of the President of the Office for Personal Data Protection over the Previous Period

From the viewpoint of the competence of the Office, last year witnessed a continued, although slow and frequently painful, *increase in public awareness of the principle of personal data protection, as part of protection of privacy* in the Czech Republic. In this relation, the public includes not only data subjects, whose data and privacy are to be protected on the basis of the Constitution and laws, but also controllers and processors, i.e. legal or natural persons responsible for data processing.

Where I mentioned that the process of increasing public awareness of the principles promoted by the Office is sometimes painful, this is caused by the fact that fines and remedial measures must be imposed in case of violation of laws. However, it can also be painful for the data subjects if they fail to protect their privacy due to ignorance of their rights and provide their personal data or consent to their use without due consideration. Intervention of the Office, if at all possible in such a case, might not provide adequate "relief" with respect to the incurred moral or material damage.

While the actual fines or remedial measures seem forceful, they are neither the objective of the Office's efforts nor the only instrument of promotion of the principles of personal data protection and dissemination of knowledge on one of the fundamental human rights and its importance for the quality of life of an individual in a democratic society. The Office strived to influence public awareness through information provided in its own publications (the Journal and Bulletin), on its website, at regular press conferences and also within an extensive leaflet campaign. Certain partial successes in increasing public awareness were also reflected in the increased number of inquiries and consultations requested during the previous term, as well as greater participation of representatives of the media at press conferences and an increased number of articles in the media, and also, on the other hand, by the greater number of complaints and instigations received. Nevertheless, the overall awareness of the controllers and data subjects can still be described as uncultivated land that will require further considerable efforts.

However, the main duty of the Office, as a supervisory body, is to handle complaints and perform controls, including both ad hoc inspections based on the received instigations and complaints and planned inspections concerned with the areas of interest of the Office. The increasing number of complaints and of the resulting in-situ inspections, other control activities and administrative proceedings is not caused only by greater awareness of individuals of their rights and potential for their enforcement, but also by an increase in and extension of the supervisory competence and the competence to impose penalties, which was implemented in 2004 in the area of birth numbers (through amendment to Act No. 133/2000 Coll., on register of population and birth numbers), and particularly also in the area of unsolicited commercial communications following from new Act No. 480/2004 Coll., on certain information society services (inaccurately called the "Anti-Spam Act"). In addition, the Act on Electronic Communications (No. 127/2005 Coll.), in the framework of which the Office performs supervision over compliance with the provisions concerning personal data processing, entered into effect on May 1, 2005. The Office had to deal with an increased number of tasks without any change in its personnel; the number of personnel should increase slightly only in the subsequent period.

The Activities of the Office were developed, and its position strengthened, not only on a national scale, but also abroad, within the global family of data protectors and partner supervisory institutions. Priority cooperation with the EU had already been developed prior to accession to the EU, when representatives of the Office were invited to meetings and events organized by the European Commission, mostly as observers. The EU funds were used to cover expenses for projects promoting achievement of the standard level of supervisory activities of the Office in certain more complex areas, including activities in the area of security and internal affairs, i.e. the Third Pillar of the EU. With accession to the Czech Republic, this cooperation improved substantially; the Office participates in meetings of advisory bodies of the European Commission, with full opportunity to present its opinions in discussions and voting and thus to participate in the creation of the common policies and common approaches and positions, which are useful for interpretation and application of the relevant rules in the Czech Republic. The international position of the Office was recognized by approval of the project of support for Bosnia and Herzegovina in the creation of a legislatively and institutionally functional system of personal data protection in the framework of the EU program to support stabilization of the situation in countries of the Western Balkan region. In that framework the Office now acts as the provider of "know-how", in collaboration with the Spanish Data Protection Agency, with which it has maintained above-standard bilateral relations practically since its establishment.

Regular international meetings of representatives of independent supervisory bodies in the area of personal data protection indicate that the conclusions of data protection agencies from the individual EU Member States and a number of other countries are very similar with respect to attempts to identify the basic areas encompassing increased risks for privacy of individuals from the viewpoint of protection of their personal data. In spite of certain historic specificities of the Czech Republic (such as, e.g., the disclosure of files of the former State Security Force, extensive use of birth numbers), the Office has come to similar conclusions on the basis of practical experience in this country. Certain phenomena, which are highly problematic from the viewpoint of personal data protection, cut across the individual sectors – they include, e.g., aspects of development of new technologies (Internet and the related services, use of biometric data, RFID technologies), introduction of camera systems, etc.

In the public sector, it is necessary to avoid an imbalanced approach to increasing public safety and State security, on the one hand, and to the fundamental rights of individuals, including the right to privacy, on the other hand. This includes especially certain ongoing, planned or discussed security measures, which are usually justified by the fight against terrorism and which tend to be gradually extended to other forms of crime, with an extensive impact on privacy of a great many persons. It must be emphasized that these are mostly innocent people who have never had and will never have anything in common with any criminal activities whatsoever. The duty of business entities to retain, over and above the scope of their usual activities, personal data of their clients, such as traffic data of providers of telecommunication and internet services, or identification data of air passengers, and disclose them to the authorities is an example of this phenomenon. Appropriateness of processing such a vast quantity of data, which can undoubtedly be misused and are also partly sensitive (e.g. location data which can constitute sensitive information under certain circumstances) has never been credibly documented with respect to the anticipated security effects. The introduction of biometric elements to travel and other documents, as another example, results, in addition to the potential misuse, in a danger of traumatizing the data subjects due to mistakes caused by imperfectness of the newly introduced equipment or technology.

With respect to the public sector, the Office believes that high risks are also related to extensive databases and central registers, from the Commercial Register and

health-care and demographic registers, to, e.g., the Land Registry, and also particularly the current tendencies to interconnect such registers and make them accessible to an increasingly large group of entities. The growing danger of misuse, including the so-called "identity theft", is evident.

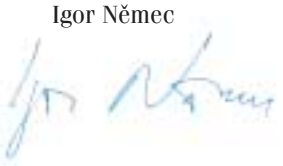
With respect to the private sector, I would like to mention two high-risk areas. These unambiguously include banking and the entire sphere of provision of financial services, including leasing. The typically weaker position of the client – natural person – on the financial market, which follows from the nature of business activities and business entities, and partially also from specific legislation, is further weakened by a certain information monopoly related to super-registers of information on debts of clients and other information on clients. Excessive application of the principle of due diligence ("Know your client"), not only in relation to registers, in combination with the aforementioned weaker position of the client, results in inappropriate requests for data. This also raises doubts with respect to the free nature of granting the data subject's consent in cases where data processing is conditional on such consent.

Increased risks from the viewpoint of personal data protection are also related to major supranational corporations, given their tendencies to transfer data of their employees and/or clients abroad and carry out their centralized processing, usually at the seat of the parent company, and often with the possibility of sharing centralized databases by subsidiaries, branches, etc. This can become a serious problem if the center of processing or the connected branches are located in countries with inadequate legislation. The usually imperfect or poorly enforceable internal regulations of the corporations mostly do not provide adequate guarantees of proper management of personal data.

In the light of the news published in the media at the end of last year in relation to the catastrophic effects of inadequate legislation in the area of personal data protection in the United States of America and the financial impact caused by this fact, there is no doubt that the attention paid to personal data protection in the Czech Republic – which is still sometimes questioned – is neither excessive nor redundant from the viewpoint of legislative efforts. In contrast, further specification of the laws, which the Office plans to bring about next year, particularly given the experience with fulfillment of the duty to punish unsolicited commercial communications and facilitate more effective performance of supervision, is based on a very detailed view of the new issues which must be confronted in order to ensure good protection of the privacy of citizens. Similar efforts will be necessary to elucidate the principles of application of the Personal Data Protection Act. Indeed, the Office continues to encounter situations where the Act is considered to be an obstacle preventing proper fulfillment of duties of, e.g., of self-governing bodies or, on the contrary, where it is used as an argument supporting the unwillingness to accept the justified demands of citizens for provision of transparent services, which is unquestionable from the viewpoint of public interest.

Moreover, with respect to the international activities and obligations of the Office in 2006, I can state with certainty that the upcoming year will be very demanding. However, I also have trust in the organizational changes which the Office has undergone and is still undergoing, as well as in the dedicated and competent work of my staff. Consequently, I am not at all concerned that the year 2006 could bring any unsolvable tasks for the Office.

Igor Němec



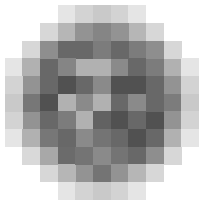
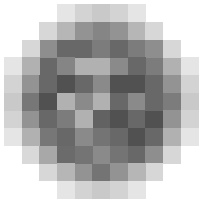


Table of contents



Activities of the Office in Numbers – 2005

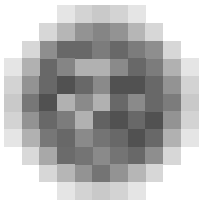
Inquiries	E-mail inquiries	1 117
	Inquiries received by mail	1 280
Complaints	pursuant to Act No. 101/2000 Coll.	408
Control activities	Total number of controls	94 + 113*
	completed	80 + 88*
	according to the plan	14
	ad hoc controls	67 + 113*
Unsolicited commercial communications	Total instigations.	1 105
	Total administrative torts	17
	Imposed fines	16
	Proceedings discontinued	2
Administrative punishment **	Total instigations received	73
	Decisions on imposing a fine	43
Registration	Total number of notifications	27 141
	Notifications lodged in 2005	1 099
	Cases of processing registered	25 054
	Controllers registered	22 128
	Registrations cancelled	735
	Number of notifications on a change in the processing	582
	Total number of applications for transfer of personal data abroad (Article 27 of Act No. 101/2000 Coll.)	684
	Decisions on authorization of the transfer of personal data abroad	625
	Decisions on rejecting the transfer of personal data abroad	16
	Proceedings discontinued on request of the party to the proceedings, pursuant to Article 30 of Act No. 71/1967 Coll.	13
	Other decisions	30
Commented legislative drafts	Acts	72
	Decrees	101
	Regulations of the Government	28
	Other	68

Institutions on whose materials (not only of legislative nature) comments were provided	Czech Mining Authority	3
	Czech Geodetic and Cadastral Office	1
	Czech Statistical Office	6
	State Office for Nuclear Safety	6
	Industrial Property Office	1
	Office of the Government	11
	Ministry of Informatics	8
	Ministry of Environment	25
	Ministry of Labor and Social Affairs	13
	Ministry of Transport and Communications	21
	Ministry of Interior	33
	Ministry of Defense	2
	Ministry of Foreign Affairs	3
	Minister of Education, Youth and Sports	20
	Ministry of Justice	17
	Ministry of Health	42
	Ministry of Finance	12
	Ministry for Regional Development	17
	Ministry of Culture	3
	Ministry of Industry and Trade	17
	National Security Office	8
Personal consultations	Consultations provided to citizens and institutions	49
Lectures, workshops	(active presentations)	42
Materials published	Journal of the Office (number of editions)	4
	Bulletin of the Office (number of editions)	2
	Positions of the Office / "On practical issues" / From decision-making of the Office	3 / 4 / 15
	Translations of foreign documents	11
	Press releases and communications for the media	13
	Additional basic documents for the media: Agency service, press, radio and television, electronic media	274
Press conferences	Regular press conferences of the Office	4
	Extraordinary	–

** Control of unsolicited commercial communications pursuant to the duty imposed on the Office by Act No. 480/2004 Coll., as amended. For more details, see p. 14)*

*** More detailed table: see p. 22*

(The table depicts the state of affairs as of December 31, 2005.)



Supervisory Activities of the Office

I. Introduction

Supervisory activities of the Office constitute the fundamental and most important field of work of this independent administrative authority. Given certain negative experience from the previous years and in relation to amendment to the Personal Data Protection Act brought by Act No. 439/2004 Coll., which established **new legal conditions** for the performance of supervision and control with effect from July 26, 2004, and also with respect to the extended competence of the Office in the area of protection of privacy in sending commercial communications, as stipulated by Act No. 480/2004 Coll., on certain information society services and on the amendment to certain other acts (Certain Information Society Services Act), a relatively fundamental organizational change took place in the Office before the end of 2004 in relation to the control and administrative tasks.

This change was also based on Resolution of the Senate No. 458/2004, recommending to the President of the Office that he carry out certain organizational measures which would improve the conditions for performance of activities of the Office's inspectors. All the aforementioned circumstances led to issuance of a new organizational regulation of the President of the Office, through which he established the ***Section of Control and Administrative Activities*** (hereinafter the "Section") as a new independent department entrusted with analysis of the received instigations and complaints concerned with infringement on the rights and duties in personal data protection, as well as with control activities directed by inspectors of the Office, and also with administrative tasks concerning first-instance decisions on imposing a sanction for violation of the Personal Data Protection Act and decisions on imposing a penalty or fine pursuant to the special law entrusting this competence to the Office. The Registration Division became a separate body of the Section, carrying out all activities related to the registration tasks pursuant to Articles 16 to 18 of the Personal Data Protection Act, as well as activities related to tasks pursuant to Article 27 of the Act, i.e. the process of transferring personal data to other countries.

Experience obtained in the work of the Section, which was established over a year ago, indicates that this step was appropriate, as it created closer links amongst the individual workplaces performing tasks within control and supervisory activities. The complexity of these activities is documented by the surveys provided below. While these are only statistical data, it should be noted that, given the personnel capacity of the Office, much greater requirements are placed on the individual employees of this Section of the Office compared to other similar authorities and, in addition to professional qualification in the areas of law and control, they must also be conversant in the field of protection of privacy as a cross-cutting topic related to a great many areas of law, both public and private. This has been negatively reflected in the relatively high fluctuation of employees of the Section, as not all these employees managed to adapt to the new working tasks

and preferred to leave the Office. On the other hand, this fact created conditions for recruitment of new employees who were not burdened by the past and accepted the new conditions and, thus, improved the current expertise of the Office.

These efforts to improve the conditions for performance of supervisory activities of the Office constitute one of the fundamental steps of the new President of the Office who had declared this intention before his election in the Senate. The fact that he has been true to his words can be proved by the subsequent steps that have already been taken or steps that should enter into effect on January 1, 2006. The first of these steps consisted in establishment of a new organizational structure of the Section in October: an entirely new separate department was created under the name ***Inspectorate***. This department is divided to four separate divisions which closely cooperate with inspectors or, more precisely, whose employees are assigned to control groups which are directly managed by inspectors performing control activities of the Office. Given the limited personnel available to the President of the Office, upon its establishment in October 2005, this department was staffed with 12 employees. However, in the framework of the second stage of organizational changes in the Office, the personnel of this department should be increased by at least 8 employees. In addition, the new President of the Office intends to establish a ***specialized workplace in Brno***, providing support for control and supervisory activities in the Moravian and Silesian regions. The President of the Office anticipates that this step should, in particular, accelerate certain administrative measures within performance of the competence of the Office, and also facilitate cooperation between the controlled entities established in this part of the Czech Republic and the Office.

Simultaneously, the President of the Office resolved to integrate the separate Legislative and Legal Departments within this Section during the first stage, resulting in new organizational arrangement of the conditions for the performance of supervisory activities of the Office. Thus, the activities of employees of the Office performing consultancy, methodical and legislative activities will be logically linked with the work of those employees of the Office who use outputs of such activities in carrying out analytical, control and administrative activities. Thus, certain shortcomings caused, inter alia, by inadequate mutual provision of information amongst the individual employees and workplaces should be eliminated in the future.

The first experience from activities of the Section carried out in the aforementioned structure indicates that there is a pressing need for mutual consultations and discussions concerned with application of legal conditions for protection of privacy under the Personal Data Protection Act and other related laws. Therefore, common ***professional workshops*** for employees of the Office are regularly organized to this end, in addition to the usual working meetings; these workshops are concerned with socially important and relevant areas of protection of privacy, such as the issues of biometric data, camera systems of subject of health cards

II. Handling of complaints

In 2005, the Office received 408 complaints concerned with violation of the Personal Data Protection Act and instigations. The aforementioned number does not include cases of suspected misuse of personal data in marketing activities carried out by electronic means which were fully examined by the Office pursuant to the Certain Information Society Services Act in 2005. These activities are the subject of the following separate part of this Report.

The problems referred to the Office by citizens in 2005 indicate the following trend, which was more apparent in the area of complaints handling compared to previous years, both in the contents of the complaints and on the basis of communication with the notifiers or injured persons, as well as in relation to the results of investigations of facts notified to the Office.

Controllers and processors of personal data are aware of the need to carefully manage personal data, at least within the extensive general framework of protection of electronic means used to process data. However, in the first place, they usually attempt to fulfill the duties related to their own procedures in personal data processing and safeguarding. Therefore, not always they pay sufficient attention to fulfillment of other statutory duties in relation to persons whose personal data are being processed, particularly with respect to the duty to provide information on personal data processing (pursuant to Article 5 (4), Articles 11 and 12 of the Personal Data Protection Act). Indeed, consent of the data subjects to processing of his/her personal data – both in cases where personal data are mandatorily required under the law and in relation to their voluntary provision – is a key precondition for proper and legitimate management of personal data. Some of the following incorrect approaches can be specifically perceived in the aforementioned conduct:

1. The individual requests for personal data from citizens create the impression that a statutory duty is being fulfilled by provision of the data, however, without clarifying the purpose and possible means of management of these personal data, and without the citizens being simultaneously expressly advised as to whether the provision of personal data is mandatory or voluntary.
2. Formalization of the consent to personal data processing, particularly through the requirement that the citizens, in addition to completing forms and questionnaires or execution of contracts, often using a special printed form, confirm the provision of their consent. The thus-expressed consent, which is often meant as an "alibi" for the personal data controller, usually cannot fully replace an advice for the citizens concerning the set purpose and manners of personal data processing.
3. Combination of several purposes of personal data processing and emphasizing the need for submitting personal data for other purposes and to other entities; however, these entities are de facto business partners of the given entity. In these cases, from the viewpoint of the Act, such persons are usually independent personal data controllers who pursue their own goals, rather than personal data processors acting for the controller who originally requested personal data on the basis of the Act or proper authorization (see Article 6 of the Personal Data Protection Act).
4. Failure to provide information on the potential processors of personal data in the framework of the information obligation pursuant to Article 11 (1) of the Personal Data Protection Act. The absence of this act results in increased concerns amongst citizens, who find that their data are held by an unknown entity, and this makes them suspect misuse of their personal data. In addition to an instigation addressed to the Office, they often lodge a criminal notice with respect to the responsible persons from amongst the personnel of the controller or processor of personal data.

In the fifth year of legal force of the Personal Data Protection Act, it is clear that a majority of members of the general public are sufficiently aware of the need to protect their privacy, actively exercise their rights under this Act and mostly do not settle for mere passive acceptance of brief information on the need to process personal data. In the work of the Office, this state of affairs is reflected

in over a third of the complaints in which intervention by the Office is requested after the controller or processor failed to satisfy the legitimate requests of the data subject pursuant to Article 21 of the Personal Data Protection Act.

In the following areas, the Office most frequently encountered suspected unauthorized personal data processing, while addressing complaints and instigations in 2005:

The importance of electronic communications has been increasing in the area of providing ***offers of goods*** and services, which is documented by a separate section of this Annual Report (see p. 14). With respect to the classical means of offering goods and services, a number of companies increasingly carry out their marketing activities from abroad; also in this case, the data subject should be aware to whom his/her data are being provided. In these cases, the Office establishes contacts with partner foreign supervisory bodies which it notifies of the suspected illegal activities.

The Office has repeatedly dealt with application of a rather problematic provision concerning the statutory requirement under Article 5 (5) of the Personal Data Protection Act, by virtue of which ***written disagreement with the offer of goods and services*** can be sent only when the addressee is already receiving loads of correspondence and advertising leaflets which (s)he has not requested. Indeed, an opposite approach is correct with respect to the Certain Information Society Services Act, as it is not possible to send electronic communications to unknown addressees, without their previous request. Effective restriction of the above-described use of personal data for offering goods and services has been supported by the new Act on Electronic Communications which enabled persons using electronic communications to reject the use of personal data contained in telephone directories for marketing purposes. The Act stipulates sanctions for failure to respect the thus-expressed will.

A number of varying complaints are lodged in the area of financial and insurance services, also as a consequence of the approach of banks to the customers which was widely discussed in 2005. Apart from comparison with the practice abroad, the objections sent by the citizens to the Office concerned particularly the following aspects: first, the behaviour of employees of financial institutions in relation to the clients and their alleged inability to answer specific questions related to the management of personal data; and second, the general and unclear contractual rules and general terms and conditions, requiring the consent to personal data processing, clearly at variance with the anticipated manner of performance of the contract (typically, the provision of a financial service is connected with the transfer of personal data abroad for an unspecified purpose). Although a number of cases notified to the Office are subjected to control, it must be stated that the contents of many objections lay partly outside the competence of the Office and rather fell within the scope of banking supervision or supervision of compliance with price regulations.

In contrast, the numerous inquiries and complaints related to the ***obligation to pay fees*** to the Czech Television constituted a very homogeneous group: 35 of those petitions were specific complaints of fee-payers who were not content with the manner of submission of their data to a private company authorized to enforce outstanding fees.

Other similar instigations received by the Office during the previous year concerned particularly the following areas:

1) Public registers. A majority of instigations and complaints are aimed against the excessive extent of publication or provision of personal data and copies of instruments containing such data. This is true, e.g., for the Commercial Register which

is still the subject of discussions related to the justification of publication of a certain group of personal data, including the birth numbers, in relation to the purpose for which the Commercial Register has been established. It is known that the published data are at least a welcomed source of data for activities of marketing companies. In 2005, the Office newly dealt with such cases with respect to the published addresses of applicants for contributions and subsidies (natural persons) whose applications for funds were not satisfied.

2) Publication of data from meetings of municipal boards and councils, particularly on the Internet. The number of complaints in this area decreased compared to 2004 after an updated opinion and guideline of the Office was issued, as the competent institutions adopted the desirable measures and the relevant personal data contained in municipal documents became accessible as stipulated by special laws providing for competence of the municipal bodies.
3) Processing of personal data in the area of municipal services. It can be stated on the basis of complaints received by the Office that, in this area, citizens are not always adequately advised of activities performed by private entities authorized by public self-governing bodies. It shows that the provision of services by public institutions to citizens necessarily entails provision of information with respect to the rights and obligations of the citizens; the right to process data must be firmly connected to the duty to advise the data subject of personal data processing.
4) Management of personal data of employees. Instigations often indicate that management of personal data could serve, inter alia, as a means of exerting pressure in resolving of labor-law disputes. Such instigations are discussed in cooperation both with Labour Offices and, where appropriate, with the newly established Labour Inspectorates (from July 1, 2005).
5) Copying of personal documents. Amendments to the Acts on Identity Cards and on Passports (effective from January 1, 2005) proved unambiguously beneficial in this respect; infractions consisting in copying of documents without the citizen's consent are now punished by municipal authorities. However, the Office continues to act in cases where a copy of the personal document is required particularly for conclusion of a contractual relationship and it also assesses the necessity and manners of use of all personal data set forth on a copy of a document, where it particularly points out that unnecessary collection of personal data could be taking place.
6) Birth number. At a time when the birth number has become an instrument and a key to a number of databases and registers without any restriction whatsoever, an amendment to the Act on Register of Population finally stipulated precise rules for the use of birth numbers. With respect to the state of affairs in the Czech Republic, Act No. 53/2004 Coll., which amended the Act on Register of Population and Birth Numbers, stipulated a transitional period to the end of 2005, during which use of birth numbers had to be brought into accordance with the law. Consequently, complaints concerned with use of birth numbers were mostly dealt with by providing an advice of the legal state of affairs effective from January 1, 2006.

Of the total number of complaints lodged in 2005, 109 were proposed and evaluated as containing grounds for commencement of investigations. In 20 cases, the notified facts constituted violation of the law that has been eventually remedied and the defective state of affairs eliminated. (cf. the table on p. 13) In those cases, the Office commenced administrative proceedings within which it assessed the degree of liability of personal data controllers or processors for breach of statutory duties or breach of the confidentiality obligation imposed on natural persons.

However, in contrast with the previous years, after amendment to the Personal Data Protection Act by Act No. 439/2004 Coll., from January 1, 2005, the Office was no longer authorized to examine violations commited by empliyees or by persons with similar status, other than those consisting in breach of the statutory duty of maintaining confidentiality of personal data. However, where a complaint consisting in notification of breach of internal procedures, evidencing primarily a labour-law violation, indicated that other statutory duties were breached (especially Article 13 of the Personal Data Protection Act), the aforementioned conduct was reviewed from the viewpoint of liability of the personal data controller or processor, or a notice was provided to the prosecuting bodies (10 notices were examined by the Office where the Office was also aware that the same matter was being investigated by the prosecuting bodies from the viewpoint of criminal liability).

Fewer instigations were concerned with areas where personal data are processed under conditions essential for the society and the State (as listed in Article 3 (6) of the Personal Data Protection Act). It is anticipated that proper use of personal data will be specified by special laws in this respect. The Office was notified of rare acts related particularly to the conduct of prosecuting bodies where, e.g., excessive personal data of a person suspected of crime were provided to the employer in the framework of investigation. Combination of data on thefts within a single file in cases, where crimes that were probably committed by a single (unknown) offender were joined, were also perceived by citizens as substantial infringement on privacy. Therefore, the relevant supervisory bodies and superior state attorney's offices were notified of the aforementioned procedures and suitability of complying with the fundamental principles of personal data protection.

Due to the above-cited amendment to the Personal Data Protection Act, the remaining tasks in the area of addressing complaints were related to petitions addressed to the courts, which were frequently of an older date – from the 1990s – and which were forwarded to the Office as the competent administrative authority after adoption of the Personal Data Protection Act in 2000. These private claims of citizens were mostly related to compensation for immaterial harm incurred in relation to unauthorized management of personal data. Similar requests for appropriate compensation by means of an apology or financial compensation are now addressed to the courts. Within its supervisory competence, the Office is obliged to concentrate on remedying the defective state of affairs by enforcing measures ensuring compliance with the statutory duties (for more details, see the Communication in Volume No. 34/2004 of the Journal of the Office).

Statistics of complaints in 2005

Instigations

– total ---------- 408

of which

– submitted for control ---------- 109

– submitted for commencement of proceedings ---------- 20

– forwarded to the competent bodies ---------- 9

– suspended with notification ---------- 173

– not suspended to date ---------- 97

III. Unsolicited Commercial Communications

As stated above, the competence of the Office was extended in 2004 to include supervision over electronic commercial communications. However, the Office commenced control activities in this area only in 2005, as the Certain Information Society Services Act did not contain any transitional period; thus, in the period shortly after this Act came into effect, the President of the Office resolved to deal with complaints delivered to the Office by mere advice on its violation.

The Act deals only with a small group of electronic communications, as specified in Article 2 (f) of the Act – the subject of commercial communications. The definition itself is a combination of positive and negative specification of this term: commercial communication means all forms of communication intended for direct or indirect promotion of goods or services or image of an enterprise of a natural or legal person, which performs a regulated activity or is an entrepreneur. Pursuant to the special regulation, commercial communications also include advertising.* In contrast, commercial communications do not include data enabling direct access to information on activities of a natural or legal person or an enterprise, particularly the domain name or e-mail address. Furthermore, commercial communications do not include data concerning goods, services or image of a natural or legal person or an enterprise, obtained independently by the user.

The regulation also applies, not only to electronic mail, but also to every text, voice, sound or picture message sent by means of an electronic communication network that can be stored in the network or in the end equipment of the user, until the user collects it. Thus, this primarily includes electronic mail, and both SMS and MMS messages, as well as, unambiguously, fax messages; the aspect of telephone calls is more complicated. If a classical telephone call, as a mutual connection of at least two parties in real time, cannot be stored, it is not subject to this regulation. However, this is not true if the call can be stored in the memory (e.g. with the use of an answering machine), both on the part of the called person and on the part of the calling person.

The scope of the Certain Information Society Services Act also excludes messages that are of a non-commercial nature. These could include, e.g. various technical notices related to unexpected changes (e.g. server failure, notice of temporary unavailability of services, etc.). However, various communications that are supposed to create the impression that a technical message is involved, but, in fact, they are part of a well-conceived marketing strategy (e.g. notices of extending the line of products or on prolonging the opening hours), must be carefully distinguished in this respect. Unsolicited commercial communications sent by persons performing regulated activities – members of professional chambers – are not subject to supervision by the Office, but rather to control ensured by those chambers.

In the spirit of Directive 2000/31/EC, the Certain Information Society Services Act provides for an exemption in relation to data allowing direct access to information on activities of a natural or legal person, i.e. particularly through the domain name or e-mail address: this information itself does not constitute a commercial communication. However, the purpose of this exemption is not entirely clear. Primarily, the Act does not specify what is to be understood under the term domain name. This is apparently only the registered domain name; however, it cannot be excluded (and such cases have already occurred in practice)

* *Act No. 40/1995 Coll., on regulation of advertising, as amended*

that the person sending such information could simply use the entire link to a website expressed through a php script. The fact that the existence of this exemption allows sending of separate messages, although with a minimum information content, admittedly poses an even greater problem.

Commercial communications may be sent to own customers on the basis of their prior consent. Such consent must meet the conditions stipulated in this respect by the Personal Data Protection Act. It must be clear that the person who granted the consent knew for what purpose, to whom and for what period the consent is granted. This opt-in principle can be briefly described in that the addressee may receive a message containing a commercial communication only if she/he has previously agreed to its sending.

Sending of commercial communications to persons other than customers of the sender is prohibited. This renders it more difficult to send such communications by specialized companies and use of various aggregated databases (mostly various corporate directories, etc.) is almost excluded. The attempts of producers of aggregated databases to ensure that their product is as perfect as possible are problematic. These databases are often offered with assurance that the entities included therein agree with the use of their contact details for the purposes of direct marketing. These databases are often acquired with the use of State subsidies, frequently even by State organizations. The aforementioned variance with the law is also caused by the fact that the Personal Data Protection Act stipulates a different principle with respect to offering goods and services than the Certain Information Society Services Act. The Personal Data Protection Act lays down the opt-out principle for marketing carried out in a manner other than electronically. This means that sending of communications is possible unless the addressee expresses his/her disagreement. However, the above-mentioned discrepancy between those laws has long been known and will be resolved this year.

As mentioned above, the Office has begun to record and examine complaints concerned with unsolicited commercial communications. For the reason of easier communication, it has established a section called “Unsolicited commercial communications” on its website, including a relatively straightforward electronic form, which allows even a person not qualified in computer technology to lodge a complaint against a sender of unsolicited electronic mail. Roughly 15 % of the approximately 1000 complaints received in 2005 were unjustified.

In case of commitment of one of administrative torts whose merits are stipulated in the Certain Information Society Services Act, a legal person is liable to a fine of up to CZK 10 million.

IV. Administrative punishment

1. GENERAL PART

New provisions of the Personal Data Protection Act concerning sanctions, adopted in the framework of amendment to that Act by Act No. 439/2004 Coll., entered into effect on January 1, 2005. A specific aspect of this amendment lies particularly in the reason for its adoption: unlike other amendments brought by Act No. 439/2004 Coll., which were caused by the need for harmonization of the Czech legislation on personal data protection with the legislation of the European Communities, amendment to the Act in the area of punishment was forced by the pressure exerted by the Ministry of Interior of the Czech Republic to unify the area of "administrative punishment" within the legislation of the Czech Republic. The longer transitional period (the remaining part of Act No. 439/2004 Coll. came into effect already in July 2004) was aimed at enabling better acquaintance with the principles of administrative punishment, including, e.g., more specific definition of merits of illegal conduct and greater diversification of the amounts of penalties depending on the gravity of infringement on the interest protected by the given rule. Thus, in 2005, the Office began to apply all these new rules in sanction proceedings which can be considered to have been a standard instrument in its activities since 2004 when these tasks were supplemented by a fundamental component of the supervisory activities of the Office, i.e. control.

In connection with amendment to substantive administrative law, which has been dealt with by the Office, as mentioned above, from the beginning of 2005, a note should also be made of the substantial change in procedural administrative law which will come into effect on January 1, 2006. Given its scope and also with respect to the number of entities (both administrative bodies and potential parties to administrative proceedings) who had to and still have to become thoroughly acquainted with Act No. 500/2004 Coll., the Code of Administrative Procedure, this Act provides for a transitional period exceeding 15 months which should ensure fluent transition to the new procedural rules without any harm on both parts. This new regulation can also be considered a challenge for activities of the Office in the coming period, not only with respect to proceedings on administrative torts, but also, e.g., in the area of registration of personal data processing or transferring personal data abroad. In its activities, the Office could particularly employ certain entirely new institutes within the general administrative process, such as order pursuant to Article 150 (1) or order issued in situ pursuant to Article 150 (5) of Act No. 500/2004 Coll., which should lead, not only to approximation of control and administrative processes, but also to their acceleration and increased efficiency in simple cases of breach of the duties of the personal data controller or processor or some other responsible person under special laws. A similar challenge for the Office could be associated with the partial amendment to Article 18 of Act No. 552/1991 Coll., on state control, following from Act No. 501/2004 Coll., amending certain laws in relation to adoption of the Code of Administrative Procedure. This amendment enables an inspector of the Office to decide that objections of the controlled entity against the control protocol would be addressed by an inspector or some other authorized officer within administrative proceedings on imposing a sanction, i.e. specifically, in that the administrative body would address the objections against the protocol in the reasoning of the decision.

Although proceedings on administrative torts related to suspected violation of the Personal Data Protection Act or Act No. 133/2000 Coll., on register of popu-

lation and birth numbers and on amendment to some related acts (Register of Population Act), are mostly instigated by the results of control activities of the Office, it must be emphasized that there are also other bodies that submit justified submissions to the Office in the above-described sense. These include particularly prosecuting bodies and municipal authorities discussing misdemeanors or other central state administrative bodies (see table p. 22). In exceptional cases, where the defective state of affairs has already been remedied or where the defective state of affairs cannot be effectively remedied by control action, proceedings may also be commenced directly on the basis of an instigation delivered to the Office by the affected data subject or some other legal or natural person, as specified in the previous part dedicated to complaints.

The number of suspected cases of violation of the Personal Data Protection Act and the Register of Population Act discussed by the Office in 2005 is given in the table (see p. 22). A special part contains description of the most important cases in which fines were validly imposed in 2005. Furthermore, it must be noted that, during 2005, the Office began to publish, in the section of the Journal of the Office called "From decision-making activities of the Office", in addition to brief descriptions of validly resolved cases in administrative proceedings, which were already provided in the information bulletin of the Office in 2004, brief quotes from decisions related to specific areas in which obligations in personal data processing are breached, in order to further increase awareness of the public of its activities and also to facilitate application of the Act by various entities which, in spite of the relatively short period of existence of the Personal Data Protection Act, are able to monitor the trends in decision-making of the Office.

The procedure of the Office in imposing sanctions was also reviewed in 2005 by the Ombudsman pursuant to Act No. 349/1999 Coll., on the Ombudsman. This review took place on the basis of an instigation submitted to the Ombudsman by a complainant who asserted that the Office failed to respond with adequate flexibility to his complaints concerning processing of personal data of his wife by her employer. The relevant complaint was one of three dealt with by the Office in connection with a labour-law dispute pursued between the wife of the complainant and her employer, where the protection of personal data was rather misused by both parties to this dispute. It followed from the conclusions of examination of this instigation, which was carried out by the deputy Ombudsman, that the Office did not make any mistakes in its action. The fact that the complainant addressed the Ombudsman with doubts concerning the correctness of the Office's procedure in relation to his instigation on the basis of recommendation from the President of the Office can also be considered to be a positive aspect, as the Office believes that review of a certain matter by an independent body can increase the trust of citizens in the Office and thus contribute to increased effectiveness of personal data protection in the Czech Republic.

The year 2005 was also the first year in which the Office imposed sanctions for dissemination of unsolicited commercial communications. As stated in the previous part of this chapter of the Annual Report, compared to the area of personal data protection, this is still a new area of competence entrusted to the Office by the Certain Information Society Services Act. Consequently, this area is primarily subject to control activities of the Office. Nevertheless, as mentioned above, the Office pursued administrative proceedings concerned with the first case of what is inaccurately called "spam". Pursuant to this special Act, the Office may impose a fine of up to CZK 10 million for dissemination of commercial communications at variance with the terms stipulated by the Certain information Society Services Act, provided that the specific amount of the fine shall be determined with respect to the gravity of the administrative tort, particularly the man-

ner of its committing and its consequences, as well as the circumstances under which it was committed (see Article 12 (2) of the Certain Information Society Services Act).

As in relation to a number of legal regulations that have recently been adopted, certain issues related to the Certain Information Society Services Act were ascertained only after it came into effect. In the area of punishment, such issues include particularly the fact that, pursuant to the Act, penalties may be imposed only on legal persons or on natural persons with respect to acts committed in the operation of their business or in direct relationship therewith, which creates a space for evasion of the Act in that natural persons, who do not operate a business and thus do not meet the aforementioned condition and are often not even employees of the given entrepreneurs, are used for sending commercial communications on behalf of certain entrepreneurs. The Office attempted to resolve this discrepancy, as well as other disputable issues, by legislative means, even though the Office as such is not authorized to lodge bills. Although the Chamber of Deputies did not approve the general intent of amendment to the Certain Information Society Services Act, the Office is now considering, in collaboration with the Ministry of Informatics, at least the potential for amending certain provisions of the Act which are the most problematic from the viewpoint of practical experience of the Office.

More detailed information on this type of proceedings is given in the table (see p. 22) and certain specific cases are described in the special part of this section.

2. SPECIAL PART

All the following administrative proceedings were pursued and ***sanctions were imposed on the basis of control findings of inspectors of the Office***.

In connection with the performance of powers of the Office pursuant to the Personal Data Protection Act, the highest fine in the previous year was imposed on a civic association which, in an attempt to bring attention to the ***subject of regulated rents***, sought for, associated and then published on its website personal data of specific tenants of apartments who, in its opinion, did not require protection provided by means of regulated rent. Identification data of the affected data subjects, including the birth number, and also sensitive personal data indicating their political preferences were processed in this manner, together with information on their real estate including lists of ownership titles and extracts from the Land Registry, including also personal data of co-owners of the real estate or other persons with rights that are entered in the Land Registry. Processing of personal data within the above scope no longer corresponded to the purpose for which the association could pursue such activity without the consent of the affected persons and without notifying them of its intent, to the extent following from Article 11 of the Personal Data Protection Act. The manner of obtaining the personal data was also at variance with the Personal Data Protection Act; *data that were obtained for various purposes*, either by own activities of the association or from a public list (Land Registry), were combined. The thus-obtained personal data were subsequently published on the website of the association, for a period exceeding one year. Furthermore, at variance with the Personal Data Protection Act, the association failed to notify the relevant personal data processing to the Office. The above-described conduct that could substantially infringe on privacy and harm the reputation of the affected persons in numerous private and public relations thereof led to breach of the duties set forth in Article

5 (1) (d) and (h), Article 11 (1) and Article 16 (1) of the Personal Data Protection Act, for which the first-instance body of the Office imposed a ***fine in an amount of CZK 550,000*** on the association in administrative proceedings; subsequently, on appeal of the party to the proceedings, this fine was confirmed by the President of the Office. In relation to this case, it must also be noted that the final decision of the President of the Office, by which he upheld the first-instance decision on an administrative tort, was contested by an action pursuant to Act No. 150/2002 Coll., the Code of Administrative Justice, which has not been resolved to date.

The Office also imposed a high fine on a ***housing cooperative*** which, in connection with the exercise of rights and obligations in administration of an apartment building, *installed and operated a monitoring system in the building*, by means of which personal data of tenants of apartments in the given building were processed without their consent. The installed cameras were operated continually and they recorded common premises of the building in such a manner that every person who entered or left his or her apartment had to pass through such premises; the resolution of the cameras was sufficient to identify persons and their activities. Electronic locks were also installed in the building, where each of the residents had a specific identifiable chip to such locks. Premises where electronic locks were installed were also recorded by cameras. Recordings from the cameras and recordings from the scanners of electronic locks constituted a comprehensive information system, with the use of which it was possible to obtain information on movement and activities of natural persons, i.e. tenants, members of the cooperative and other visitors, on the common premises of the building. The recordings from the monitoring system were systematically transformed to digital files, marked with location and temporal data and stored on a data carrier for the purpose of their use as means of evidence in activities of the bodies of public administration. Given the comprehensive nature of the installed system, it was not possible in the given case to refer to the provisions of Article 5 (2) (e) of the Personal Data Protection Act which permits personal data processing without the consent of data subject in cases where this is necessary for the protection of rights and legitimate interests of the controller, as the employed means and manner of personal data protection were not appropriate to the extent and manner of endangering of the rights of the cooperative or its members. Thus, the cooperative could have adopted the aforementioned measures only with the consent of the residents of the building, while simultaneously advising all persons entering the building of the fact that the common premises of the building are being monitored by cameras.

The combination of recordings from the camera system with the recordings from scanners of electronic locks resulted in substantial and unjustified infringement on private and personal life of the data subjects, which had to be assessed as violation of the Personal Data Protection Act and which could also be considered to be at variance with Art. 8 (1) of the Convention for the Protection of Human Rights and Fundamental Freedoms which is, by virtue of Art. 10 of the Constitution of the Czech Republic, part of the legal order of the Czech Republic and has priority over laws. Indeed, according to the European Court for Human Rights, premises outside dwellings, such as common premises inside a building, must be considered to be private premises, as limiting privacy only to the inner area where an individual can live his or her private life according to his wishes would be an excessively strict interpretation. The right to protection of private and personal life of affected data subjects is infringed by monitoring the residents of the building and their visitors upon entering or leaving the building. The above-described continual monitoring connected with further temporally unlimit-

ed storage of the acquired recordings cannot be considered to be lawful with respect to the aforementioned reasons. By the above-mentioned conduct, the housing cooperative breached the duty stipulated in Article 5 (2) of the Personal Data Protection Act, as the camera system was installed without consent of the residents of the building; a ***fine of CZK 180,000*** was imposed on the cooperative for this administrative tort. In relation to this case, it must also be noted that the final decision of the President of the Office, by which he upheld the first-instance decision on an administrative tort, was contested by the cooperative through an action pursuant to Act No. 150/2002 Coll., the Code of Administrative Justice, which has not been resolved to date.

Another fine was imposed on the ***armed force of the Czech Republic*** in relation to *scanning of biometric data and pictures of fingerprints*. Data on fingerprints were routinely acquired at variance with the special laws regulating the procedure of the armed force also with respect to persons who did not meet the requirements for permitted taking of fingerprints, as specified by the special laws, and, moreover, data on fingerprints were not processed separately within the performance of various tasks of the armed force. The special law requires that the armed force also verify, at least once every three years, whether the processed data are further needed for the fulfillment of its tasks, which is related to the duty stipulated by the Personal Data Protection Act to destroy personal data after expiry of the period required for their processing. The date, from which the period limiting the necessity of further personal data processing begins, was not set due to a methodical error; thus, the information systems also contained data on fingerprints where the period of their processing on the basis of the Act has already expired. Furthermore, it was proved that *the purpose, for which the data on fingerprints are to be collected* pursuant to the substantively applicable laws, was not in conformity with the purpose of processing that was actually pursued in the collection of and search for (ascertaining of) data on fingerprints of the individual natural persons. This discrepancy consisted in the fact that the data on fingerprints that were stored in the information systems were also used for other purposes. The frequency of cases of breach of this duty, as ascertained within the examined sample of audit records, indicated that this was a very common, if not general, practice.

This conduct led to breach of the duties stipulated in Article 5 (1) (d), (e) and (f) of the Personal Data Protection Act, for which ***a fine of CZK 100,000*** was imposed on the given personal data controller, particularly due to the fact that the data on fingerprints are partly biometric data which are sensitive in the sense of Article 4 (b) of the Personal Data Protection Act and require increased protection.

The Office also imposed high fines within the performance of its new competence pursuant to the Certain Information Society Services Act. This competence covers the area of sending unsolicited commercial communications, inaccurately called “spam”.

The highest fine in connection with sending commercial communications in the sense of Article 2 (f) of the Certain Information Society Services Act was imposed on a company that *used electronic means to disseminate unsolicited commercial communications* with an offer of free presentation in the database of business entities located at a specific internet address, without having obtained demonstrable prior consent of the addressees to the sending of the commercial communication. The given company sent unsolicited commercial communications on the basis of an contract for addressing clients, in which it agreed to address, during a certain period of time, a certain number of business entities with an offer of products of another company. Under the contract, the

company was to address potential clients through an e-mail address that was established for this purpose; it was responsible for obtaining e-mail addresses, as well as for their legitimate use. The communication also included a request for expressing the consent to or disagreement with sending the offer. However, pursuant to Article 7 (2) of the Certain Information Society Services Act, in order for it to be possible to send a commercial communication to a person whose e-mail address has been obtained as from a customer of a company, whose services or goods are to be presented by means of the commercial communication, it is necessary to obtain demonstrable consent of the given person to the use of his/her e-mail address for this purpose. Logically, the consent must be provided prior to sending the actual commercial communication. In this case, it is permissible to send a communication that does not promote goods, services or image of a natural or legal person, but rather only contains a question whether the addressee is interested in sending a commercial communication concerning products of a certain company. Only an unambiguously positive answer (rather than silence) can be considered to constitute consent in the sense of Article 7 (2) of the Certain Information Society Services Act. However, in the given case, the *communication that was sent already contained an offer of a certain product.* Any subsequent statement of the addressed persons based on a request contained in the wording of the relevant commercial communication cannot be considered to be consent pursuant to Article 7 (2) of the Certain Information Society Services Act.

The above-described conduct led to breach of the duty stipulated in Article 7 (2) of the Certain Information Society Services Act and, thus, to commitment of an administrative tort pursuant to Article 11 (1) (a) of the Act, for which ***a fine of CZK 160,000*** was imposed on the company. The party to the proceedings lodged a remonstrance against the decision on the fine; however, it was rejected because it was late.

3. REVIEW OF ADMINISTRATIVE DECISIONS OF THE OFFICE

Decisions made by the Office in two aforementioned cases were challenged by an administrative action during 2005; a decision has not yet been made on these actions. Two cases from 2004, as well as one case from 2002, are still pending. The above-mentioned oldest unresolved case is concerned with a financial institution that was not able to effectively protect personal data of its clients and whose electronic equipment containing records of personal data of several hundreds of thousands of clients was stolen. The decision of the Office on imposing a fine was contested by an action of 2003, which was rejected by the Municipal Court in Prague in 2004, thus upholding the decision of the Office. The financial institution then challenged the decision by a cassation complaint which, however, has not been decided on by the Supreme Administrative Court to date.

Another case which is still pending before the courts is a decision of the Office through which it refused to grant a natural person the status of a participant in administrative proceedings held in 2004. The affected person lodged an administrative action against this decision, which was rejected by the Municipal Court in early 2005, whereby, as in the previous case, it upheld the decision of the Office. This decision was also contested by a cassation complaint which has not been decided on by the Supreme Administrative Court to date.

The last case of 2004 is concerned with a decision of the Office on imposing a fine for unauthorized personal data processing in connection with resolutions of the council and board of a city that were published in full wording (i.e. without

respecting personal data protection) on the website of the municipal authority. In October 2004, the decision of the Office was challenged by an administrative action which has not been dealt with by the Municipal Court in Prague to date.

4. NUMBER OF INSTIGATIONS AND PROCEEDINGS HELD

Number of instigations concerned with a suspected administrative tort pursuant to the Personal Data Protection Act and the Act on Records of the Population

Total ---------- 73
of which:
– on the basis of control activities of the Office ---------- 28
– by referral of the matter by the prosecuting bodies and bodies dealing with misdemeanors ---------- 14
– on the basis of an instigation from natural and legal persons ---- 31
Addressed:*
– through discontinuation prior to commencement of proceedings -------- 8
– through a decision on imposing a fine (total) ---------- 43
– of which:
– with legal force ---------- 36
– by discontinuation of proceedings ---------- 9
– by an official record after commencement of proceedings ------- 2

** Including addressing of instigations, whose discussion was commenced in 2004.*

Number of instigations concerned with a suspected administrative tort pursuant to the Certain Information Society Services Act

Total ---------- 18
Addressed:
– through a decision on imposing a fine (total) ---------- 10
– of which:
– with legal force ---------- 6
– by discontinuation of proceedings ---------- 2

V. Registration

The reorganization of the departments of the Office pursuing control and administrative tasks, which is described in more detail in the introduction to this section of the Annual Report and which entered into effect on October 15, 2005, resulted in no substantial changes with respect to the activities and status of the Registration Division. The Registration Division, which was separated from the Department of Administrative Decision-Making within the previous reorganization with effect from December 1, 2004 and, at the same time, incorporated in the newly established Section of Control and Administrative Activities, continues to have this status. The main object of activities of the Registration Division continues to include full competence in the area of assessing individual notifications of personal data processing pursuant to Article 16 and permitting the transfer of personal data to other countries pursuant to Article 27 of the Personal Data Protection Act.

1. REGISTRATION ACTIVITIES OF THE OFFICE

With respect to registration procedures, the Office concentrated in 2005 particularly on the following areas:

- creation of the new design of registration forms that would provide more comprehensive information on the given processing, particularly with respect to specification of its purpose;
- publication of comments on processing that is not covered by the notification obligation, but whose registration is often required by the controllers;
- preparation of a new database system of the register, including introduction of acceptance of notifications in an electronic form.

It has become almost a matter of fact that the ***notification obligation is fulfilled by the controllers (notifiers) through registration forms*** which were created immediately after establishment of the Office in order to facilitate the registration obligation of the controllers. With respect to the developments in the area of personal data protection during the five years of existence of the Office and on the basis of experience to date, it has been found necessary to update the registration forms and specify the required information so that the accepted notifications are processed more flexibly and also that the registration forms are more comprehensible for the controllers (notifiers). It follows from various inquiries and accepted notifications that the notifiers encounter considerable problems in completing the registration forms, particularly with respect to determining the actual purpose of processing, and that there are many unnecessary misunderstandings. In relation to the notifiers, the Office strived to make the registration form as comprehensible as possible, while simultaneously facilitating the fulfillment of the notification obligation by the anticipated introduction of electronic acceptance of notified cases of processing. From the viewpoint of the needs of the Office, *new registration forms should allow identification of new types of processing which are introduced together with the development of modern technologies (chip cards, processing by camera systems, etc.)*, as well as the increasingly frequent processing of a more extensive scope of personal data, e.g. biometric and genetic. Introduction of a new registration form will also place higher demands on analysis and evaluation of the obtained information. On the other hand, it can be expected that it will be pos-

sible to obtain more comprehensive information on the registered cases of processing from the register of processing on the basis of notifications pursuant to the new registration form, which will also contribute to more effective work in the area of control activities of the Office.

Similar to 2004, the ***trend of gradual decrease in the number of notified cases of processing*** continued in 2005. However, simultaneously, as in 2004, the individual notifications were assessed in more detail compared to the previous years. An accepted notification is analyzed in the framework of the registration process particularly from the viewpoint of specification of the purpose of processing; it is assessed whether the scope of personal data, especially of sensitive data, is appropriate to the set purpose; and, last but not least, the actual nature of processing is analyzed with respect to the exemptions pursuant to Article 18 of the Personal Data Protection Act or with respect to distinguishing between the controller and processor. Registration proceedings pursuant to Article 16 (4) of the Act were commenced with respect to almost half of the received notifications.

The most frequent reasons were as follows:

Suspected notification of personal data processing by the processor

The processor continue to submit notifications, although amended Article 16 (1) of the Personal Data Protection Act now clearly imposes the registration obligation only on the controller and, thus, the notification obligation does not apply to the processor. This is caused by the fact that, prior to commencement of personal data processing, the notifiers are not able to determine whether they are in a position of personal data controllers or merely processors and prefer to send the notification to the Office. It is important to distinguish between the controllers and the processors particularly from the viewpoint of division of responsibility for certain processing. Many notifiers assume the role of a controller, although in fact they are not in such a position. This issue is often resolved only during the registration proceedings and it is noted that the given case entails personal data processing by a processor, who is not subject to the notification obligation. From the total of notifications submitted by processors to the Office ***22 % were submitted by virtue of misunderstanding***, because the processors were insurance agents, business agents, brokers and other persons pursuing similar activities. Position of the Office No. 1/2005 (Activities of insurance intermediaries and the notification obligation) was published on the website of the Office in this respect. It follows from the above-described facts that distinguishing between the controllers and processors, as defined by the Personal Data Protection Act, still causes considerable problems.

Suspected notification of processing pursuant to Article 18

Similar to 2004, a number of notifications lodged in 2005 were concerned with processing that was not subject to the notification obligation due to the fact that such processing met the precondition for exemption from the notification obligation pursuant to Article 18 (1) (b) of the Personal Data Protection Act. Pursuant to that provision of the Act, it is not necessary to notify the Office of personal data processing imposed on the controller by special laws or processing required for exercising rights and obligations following from special laws (mostly processing in the area of social care, education, health care, employment, activities of territorial self-governing units, civic associations, housing cooperatives, etc.). Unfortunately, a great many controllers still incorrectly believe that each case of processing must be notified to the Office. Another reason consists in the fact that

certain controllers are not able to sufficiently assess whether they process personal data pursuant to Article 18 (1) (b) of the Act. Given the fact that it is not the objective to register notifications that need not be registered pursuant to the law, areas of processing to which the notification obligation usually does not apply are published in the Journal of the Office and on the website of the Office in order to improve understanding of this issue. Comments have been published to date in relation to personal data processing by insurance agents and business agents, processing of personal data of employees for the purpose of performance of tasks in the area of personnel and salaries, personal data processing by territorial self-governing units and personal data processing by institutes of social care. These activities should raise awareness of the controllers (notifiers), as well as awareness of personal data protection in the area of registration activities, and also reduce the administrative load following from "unjustified notifications". The number of the above-described notifications equaled approx. ***13 % of the total number of accepted notifications*** in 2005. If the registration proceedings lead to the conclusion that the given processing is not subject to the notification obligation, this fact is communicated to the notifier by a letter.

Other reasons for commencement of registration proceedings included failure to state the purpose of processing (6.7 %), submission of an incomplete notification (3 %) and suspicion of violation of the law in relation to notification of processing of sensitive data (2 %), e.g., with respect to the inappropriate scope of personal data in relation to the purpose of processing.

In connection with a change in the registration process resulting from amendment to the Personal Data Protection Act by Act No. 439/2004 Coll., it was also necessary to make a ***change in the database system of the register*** which provides for all circulation, processing and keeping records of the received notifications of processing and other written documents in electronic form. Partial changes and modifications of the current system have been carried out in this respect to date, where first steps have been taken to create an entirely new database system of the register, which is a basic precondition for more effective work in electronic data processing. The delays in this respect were caused, more or less, by circumstances that led to modification of registration forms. This is also related to the anticipated introduction of electronic acceptance of notifications of processing, which should contribute to a more effective process of acceptance of notifications, as well as to more straightforward fulfillment of the notification obligation by the controller (notifier).

2. FREQUENT MISTAKES IN RELATION TO THE REGISTRATION OBLIGATION

Frequent inquiries made by the controllers indicate their ***lack of awareness*** of issues related to the purpose of keeping the registers or to questions like "what does an entry in the register indicate?". First, it should be emphasized that the duty to keep the register of personal data processing is imposed on the Office by the Personal Data Protection Act in Article 29 (1) (b), similar to the duty to make the register available to the public (except for information stipulated in Article 16 (2) (e) and (i) of the Act), particularly in a manner enabling remote access (Article 35 (2)). The register constitutes records within the usual meaning, containing cases of personal data processing notified by the controllers in the Czech Republic, except for those cases of processing that are not subject to the notification obligation on the basis of statutory exemptions stipulated in Article 18 of the Personal Data Protection Act. As the register is publicly accessible, also in electronic form on the website of the Office, it should also serve as general information for data subjects indicating which personal data are processed and for what purpose. Of course, the register is also used for internal needs of the Office, particularly for the purposes of control activities.

If interested, the controller may request that the Office issue a ***certificate of registration*** pursuant to Article 16 (5) of the Personal Data Protection Act. However, it must be noted that the registration process pursuant to Article 16 of the Act is not a permitting process and that the issued certificate only documents that the controller has fulfilled his statutory obligation to notify the Office of intended processing and that the processing is recorded in the register kept by the Office. Indeed, the controllers often use the certificate of registration to prove that their processing has been verified by the Office and is, therefore, in absolute conformity with the law. In this respect, it should be noted that registration of notified processing is carried out only on the basis of facts available and known at the given time. The registration process cannot simply replace control performed in situ, which is the only means of proving that such processing is in accordance with the law. Thus, it must be pointed out that, by making an entry in the register or issuance of a certificate of registration, the duties of the controllers (notifiers) following from the Personal Data Protection Act are not waived. These duties must be fulfilled during the entire term of personal data processing.

The objective of the registration proceedings is to determine notifications raising a justified suspicion that personal data could be processed at variance with the law, and also that selected groups of sensitive data could be subject to processing or that certain types of processing could pose an increased risk with respect to the rights and freedoms of data subjects. Another objective is to provide guidelines for the controller with respect to any anticipated processing prior to its commencement. The above-described process leads, inter alia, to partial elimination of illegal procedures in personal data processing, e.g., by modification of the scope of personal data for the declared purpose. It must also be noted that *it is widely considered that the Office keeps a register of controllers, rather than a register of processing, which is not true*. Thus, rather than the controller himself, the relevant processing carried out by the controller is the primary subject of registration assessment and the subsequent entry in the ***register of personal data processing***.

Misunderstanding is frequent in ***processing of sensitive personal data***. Sensitive data on nationality, race or ethnic origin are often confused with personal data on state citizenship which are not sensitive in the sense of Article 4 (b) of the Personal Data Protection Act. An extract from the Criminal Records proving

lack of criminal record also does not constitute sensitive data concerning conviction of a natural person of an offense in the sense of the above-cited provision. Some employers believe that they process sensitive data on the health condition of their employees. A certificate issued by a physician or a health-care facility (e.g. within an initial or preventative medical examination), according to which an employee is or is not able to perform his/her work, is not sensitive data on his health condition in the sense of the Act. Thus, sensitive data on the health condition of employees may be processed, e.g., only by the internal doctor, but not by the employer. Employment of employees with a modified working capacity could be an exception in this respect. In this case, obligations of the employers related to employment of disabled employees are stipulated by special regulations.

Intention to process personal data by means of ***monitoring camera systems*** was more frequently notified in 2005. Certain cases notified to the Office involved more than simple monitoring of a certain building (e.g. manufacturing area) or a movable thing (e.g. technical equipment) aimed at prevention of damage, loss or unauthorized manipulation. The Office was also notified of intended monitoring of employees at workplaces (in workshops, production halls, warehouses and even cloakrooms). Of course, in the latter case, which involves a clear 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 rejection of personal data processing. However, more often the controller agrees to reduce the originally intended scope of personal data or to make other modifications of the contemplated processing.

The number of notified cases of ***processing of biometric data*** is also increasing. Processing of biometric data is often used in automated procedures of verification and identification, especially for control of entry to both physically existing and virtual areas (e.g. access to certain electronic systems or services). Processing of biometric data consisting in voice recordings and fingerprints for the purpose obtaining access to computers and networks was notified in several cases during the year. Casting agencies which keep records of the applicants, e.g. for television, film or advertising production, are another example in this respect. These agencies process biometric data, such as height, weight, color of eyes, hair, etc.

3. TRANSFER OF PERSONAL DATA ABROAD

In relation to decision-making on applications for authorization to transfer personal data to other countries, it can be stated that, compared to 2004, there were substantially fewer applications containing incomplete or inaccurate information or applications not accompanied with the necessary documents from which the Office could reliably determine the actual state of affairs. When assessing each request, various circumstances are taken into consideration. A key question is always whether the legislation of the country of destination provides adequate safeguards for personal data protection. If the national legislation in the given country cannot be considered to be adequate, it is necessary that one of the conditions stipulated in Article 27 (2) and (3) of the Personal Data Protection Act is met for the transfer of personal data. Prior to issuing each decision, the Office also assesses other aspects of the application – it deals particularly with the purpose of processing personal data, their source, final destination and period of processing.

Recent applications lodged by legal persons were concerned especially with ***transfers of personal data*** of employees or applicants for employment to parent companies abroad, particularly in the United States of America. The most fre-

quent reasons were stated as follows: common management of personal policies, planning of personal development of employees, more effective use of human resources, planning of further education of employees and tasks related to settlement of expenses incurred during business trips and travels.

In several cases, the applications were irrelevant, as an agreement on transfer of personal data had been concluded between the applicant (exporter of personal data) and the recipient of personal data in a third country, including the ***contractual clause*** pursuant to the Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC. Indeed, the requirements were met in these cases for the transfer of personal data under the regime specified in Article 27 (2) of the Personal Data Protection Act, according to which personal data may be transferred to third countries if the prohibition of restriction of the free movement of personal data is ensuing from an international treaty to the ratification of which the Parliament has given his assent and which is binding the Czech Republic, or if the personal data are transferred on the basis of decision of an institution of the European Union. Thus, in these cases, it was not necessary to apply to the Office for authorization pursuant to Article 27 (4) of the Personal Data Protection Act, as the Office is not competent to make decisions on such authorization.

Some applications that were concerned with the transfer of personal data to the United States of America were subject to Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the ***safe harbour privacy principles*** and related frequently asked questions issued by the US Department of Commerce (Safe Harbor cases). In this case, an adequate level of personal data protection in their transfer to the United States pursuant to the aforementioned decision can be attained if the recipient of personal data in the U.S. would adhere to the safe harbor principles for personal data protection, as well as the principle of frequently asked questions (FAQ) represented by the guidelines for the performance of these principles issued by the Government of the United States of America on July 21, 2000. *Two fundamental preconditions must be met in each transfer of data: the recipient of the data has unambiguously and publicly committed to adhere to the principles performed in accordance with FAQ and, simultaneously, this entity is subject to the statutory powers of the public administrative body of the United States of America* (the Federal Trade Commission or the Department of Transportation of the United States of America) which is authorized to investigate on complaints in case of non-adherence to the principles performed in accordance with FAQ and provide for a remedy against unfair or misleading practices, as well as indemnification for natural persons, irregardless of the country of their residence or nationality.

The Office also dealt with an application concerned ***with provision of personal data of travelers*** from the APIS system that were to be submitted to the United States' Bureau of Customs and Border Protection by an air transport company operating international passenger flights to the United States of America. As this aspect is provided in detail in the Commission Decision 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 Office stated that the transfer of personal data to the United States of America would be implemented on the basis of the above-cited decision of the body of the European Union and, therefore, it was not necessary to apply for a decision on authorization to transfer personal data to third countries. Article 27 (2) of the Personal Data Protection Act also applies to this specific case.

Statistics of notifications of processing of personal data pursuant to Article 16

	Total figures as of Dec. 31, 2005	in 2005	in 2004	in 2003
Total number of notifications	27 141	1 099	1 972	3 187
Cases of processing registered	25 054	466	1 591	2 854
Controllers registered	22 128	419	1 402	2 604
Registrations cancelled	735	111	64	52
Number of notifications on a change in the processing	582	134	192	216

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

	Overall figures as of Dec. 31, 2005	in 2005	in 2004	in 2003
Total number of applications	684	41	52	89
Decisions on authorization of the transfer of personal data abroad	625	37	60	69
Decisions on rejecting the transfer of personal data abroad	16	0	0	1
Proceedings discontinued pursuant to Article 30 of Act No. 71/1967 Coll. on request of the party to the proceedings	13	0	3	6
Other decision	30	3	0	0

VI. Activities of the Office in the Legislative and Legal Area

POSITION AND COMPETENCE OF OFFICE

The position and competence of the Office, as an independent supervisory body of the state, is defined by the Personal Data Protection Act. In 2005, the Personal Data Protection Act was affected by two direct amendments and it is therefore currently valid as amended by laws adopted during the previous years, i.e. as amended by Acts No. 227/2000 Coll., No. 177/2001 Coll., No. 450/2001 Coll., No. 107/2002 Coll., No. 309/2002 Coll., No. 310/2002 Coll., No. 517/2002 Coll., No. 439/2004 Coll., No. 480/2004 Coll., No. 626/2004 Coll. and, newly, with effect from January 1, 2006, also Act No. 413/2005 Coll. and Act No. 444/2005 Coll. Part Forty-Four of Act No. 413/2005 Coll., on amendment to laws in relation to adoption of the Act on Protection of Confidential Information and Security Qualification, contains direct amendment to the Personal Data Protection Act. This is a minor, in fact legislatively technical, amendment, by which the word "facts" in Article 37 (c) is replaced by the word "information" and footnote No. 31 containing reference to Act No. 412/2005 Coll., on protection of confidential information and security qualification, is added. The other amending law is Act No. 444/2005 Coll., amending Act No. 531/1990 Coll., on territorial financial bodies, as amended, and some other laws. Part 28 of that Act amends Article 46 (7) of the Personal Data Protection Act in that the words "territorial financial authority" are replaced by the words "customs authority".

In 2005, the Office was entrusted with new competence in the area of ***supervision of personal data protection in the field of electronic communications*** following from Act No. 127/2005 Coll., on electronic communications and on amendment to some related laws (Act on Electronic Communications). Pursuant to Article 87 (4) of that Act, supervision over compliance with the duties in personal data processing is entrusted to the Office for Personal Data Protection. This is based on the obligations of the Czech Republic to implement EU Directives in this area, where, in addition to regulatory telecommunication authorities which have also traditionally acted as supervisory authorities, competence related to compliance with duties in personal data processing is entrusted to special authorities – i.e., in the Czech Republic, to the Office for Personal Data Protection. In addition to the basic scope of competence of the Office pursuant to the Personal Data Protection Act, the Office also maintains competence stipulated in 2004 (by amendment to Act No. 133/2000 Coll., on records of the population and birth identification numbers and on amendment to some laws, as amended, implemented by Act No. 53/2004 Coll., amending some laws related to the area of records of the population) in cases of unauthorized management of birth identification numbers or authorized use of birth identification numbers; pursuant to the Certain Information Society Services Act, the Office also performs, within the defined scope, supervision over the decision-making activities related to breach of duties of responsible entities in the area of unsolicited commercial communications.

1. ACTIVITIES OF THE OFFICE IN THE LEGISLATIVE AREA

A Government regulation was prepared at the end of 2004 in accordance with the wording of the amendment to the Personal Data Protection Act (Act No. 439/2004 Coll.), ***concerning the form of the service card of inspectors and other control workers***, who will be obliged to prove their identity through these cards within controls carried out by them. The duty to prepare and issue this regulation follows from the authorization in Article 38 (5) of the Personal Data Protection Act in the valid wording. The Office has fulfilled this plan and the Government Regulation concerning the form of the service card of employees of the Office performing control was published in the Collection of Laws under No. 8/2005 Coll.

The Office participated, as usual, in the governmental legislative process as an obligatory commentary place in preparation of legislation drawn up by other institutions in the framework of the governmental legislative process in cases where such proposals affect the area of personal data protection. Thus, during 2005, the Office could provide comments on more than 200 draft legal regulations of various legal force. However, the number of comments raised by the Office documents that the drafting parties do not pay adequate attention in drawing up the draft legislation to the principles of personal data protection and the drafts often lack basic requirements of the Personal Data Protection Act, such as an accurately specified scope of personal data, clearly defined purpose and manner of personal data processing, specification of the period required for their storage, etc. The authors of the legal drafts (particularly of implementing regulations) still tend to evade the authorization stipulated in laws and, e.g., set a wider scope of data than expected with respect to the purpose of processing.

Of all the commented legislation, attention should be given to two regulations. The first, if adopted by the Parliament of the Czech Republic, will have a fundamental impact on use of one of the most extensive public administrative registers – the records of the population. The draft Act amending certain laws related to the area of records of the population has been drawn up by the Ministry of Interior in response to a situation where, in the opinion of the drafting party, the current legal regulation is inaccurate and often difficult to apply. In cooperation with the Office, it was possible to find a solution that corresponds to the principles of personal data protection in that, while the precise scope of data that can be drawn from the system of records of the population and further used for the performance of statutory tasks is set for the individual authorized entities, this scope is defined as a maximum, provided that only data that are required for the performance of tasks may be used in each individual case. Thus, it should not always be possible to use, automatically and without justification, all data that could theoretically be disclosed or submitted to the individual authorized entities.

The second above-mentioned commented regulation will also have direct impact on the citizens. Again, this is a policy of the Ministry of Interior; however, this regulation is based on implementation of the legislation of the European Union which imposes the introduction of biometric data to travel documents. The draft Act amending certain laws in the area of travel documents contains amendments to several laws and was drawn up to transpose Council Regulation No. 2252/2004 (hereinafter the Regulation). The Regulation requires that the EU Member States introduce, under the set conditions, introduce to passports and travel documents a storage medium containing a facial image and, eventually, also fingerprints in interoperable formats. In this case, the comments of the Office were again aimed at implementing the above-cited Regulation, while simultane-

ously respecting EU 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. The primary objective of the comments of the Office was to ensure that the scope of processed fingerprints is not extended over and above the necessary framework, as defined by the above-cited Regulation, and also to assure citizens – holders of travel documents – that these data would be verified in an appropriate manner upon issue of travel documents. That should simultaneously ensure that the draft legislation will not be contrary to the conditions and principles of personal data protection as stipulated by the Personal Data Protection Act. The Act amending certain laws in the area of personal documents should also establish another area of competence of the Office consisting in supervision and imposing sanctions in the field of protection of privacy in personal data processing. The competence of the Office should include discussion of misdemeanors and administrative torts consisting in unauthorized processing of biometric data processed in a data carrier containing biometric data.

Finally, it can be stated that, although the Office was not able to enforce certain comments in the framework of the legislative process in the Czech Republic, such as, e.g., in relation to the new regulation of the conditions for collection of the radio and television fees, it can be stated that further gradual steps were made in the Czech Republic in 2005 to the overall harmonization of the legislation of the Czech Republic with the principles of personal data protection.

2. ACTIVITIES OF THE OFFICE IN THE AREA OF GENERAL APPLICATION OF LAW

The interest of the general public, as well as of individual controllers and processors of personal data, in provision of standpoints, consultations and discussions concerning application of the Personal Data Protection Act in the framework of the legal order of the Czech Republic continued in 2005. In the framework of these activities, the Office provided over ***4 000 telephone consultations***, which corresponds to an increase of more than 30 % compared to 2004 and almost 60 % compared to 2003, and addressed more than ***1 000 written*** requests (and over 1 000 requests sent by electronic mail). The increase in the number of requests for consultations lodged by electronic mail document that the public is interested in obtaining quick or informal answers or advice as to how they should proceed in specific and current cases.

At the beginning of 2005, a major part of consultancy provided by the Office for Personal Data Protection was still concerned with inquiries related to proper application of the competence related to unsolicited commercial communications pursuant to the Certain Information Society Services Act and opinions of the Office in this respect. In this relation, the Office continued to present its positions and also published these positions on its website. It appears that this subject has already been comprehended by the professional public and the number of inquiries in this relation has also been decreasing. It can also be stated that the aspect of use of birth identification numbers has already been adequately clarified and this topic has been less frequently raised in requests for consultations and application approaches than in 2004. However, it can be stated that, in turn, the range of issues concerning directly the interests of the general public has increased; i.e. more frequently the Office is inquired or requested to make a statement on issues that are characterized by the question "… is it possible that?". Questions of this type are concerned with numerous areas of everyday life, where a considerable part is related to certain practices of banks and other financial institutions. Certain activities of these entities and their attempts to obtain infor-

mation seems excessive to a major part of the population and is even perceived as infringement on their privacy. However, the problem lies in the fact that the relevant institutions use an approach in that they make provision of a service itself conditional on obtaining information or granting consent to further processing of personal data.

Similar notes could made in relation to, e.g., *providers of telecommunication services* who relatively often use methods consisting, e.g., in amendments to the general terms and conditions which, however, entail the consent to processing of personal data and their further use for the needs of telephone operators in such a manner that the client or potential client cannot refuse if she/he wants to use the service. The opinion of the Office in this relation is unambiguous: such practices must be changed and the principle of consent to data processing must be applied so that its statutory contents are fulfilled, being defined as a free, conscious and informed manifestation of will, i.e. as a legal act of the data subject towards the entity that requires such consent for personal data processing.

A substantial part of interpretation of application approaches by the Office was concerned with answering questions raised by *city and municipal officials*. These questions are mostly related to issues of correct application of special legal rules in connection with the Personal Data Protection Act. On the basis of analysis of these issues, it can be concluded that, in a number of cases, the only step required lies in modification of the well-established routine procedures, whereby any further problems entailed in processing and use of personal data are eliminated. The Office is also frequently asked for an opinion on proper application of Act No. 106/1999 Coll., on free access to information. The problem lies in the fact that, except for the published case-law of general courts, there is practically no official institution (administrative authority) in the Czech Republic that would facilitate normal practice by its opinions and employed application approaches. However, in this case, the Office can only express its opinion, in which it must, moreover, take account of the correct application of the Personal Data Protection Act. However, the responses indicate that even such information and opinions are of benefit for the inquiring parties.

The Office was newly addressed by the prosecuting bodies in relation to investigation of criminal offenses pursuant to Article 178 of the Criminal Code, i.e. unauthorized management of personal data. The Office is either addressed by means of a request for an opinion pursuant to Article 8 (1) of the Code of Criminal Procedure or, more frequently, it is asked for a professional opinion in the sense of Article 105 of the Code of Criminal Procedure. It can be derived that the increasing number of the latter requests indicates, on the one hand, that the professional expertise of the Office is respected, and on other hand, that there is also an increasing number of offenses of unauthorized management of personal data. This could lead to a justified conclusion that the influence of the Office over the general public is beginning to show results and that the citizens increasingly protect their privacy, also under criminal law.

A new feature of consultancy is also related to the attempts of the applicants to notify the Office of the intention to process personal data already in an early stage of preparation of the project. This is evidenced by the history of preparation and the subsequent implementation of projects of client information systems of banks and a number of other databases of clients. The prior consultations of the authors and implementing bodies with the Office serve as a certain guarantee that their approach is correct. Similar, some future controllers or processors addressed the Office in 2005 with their plans and asked for consultations. Although the Office, aware of its exclusive position in the area of supervision,

cannot refuse a consultation with reference to the possible later control, the employees of the Office who provide the relevant consultations attempt to deal with the authors and implementing parties in open terms and to persuade them to make the necessary changes in their approaches which are unacceptable from the viewpoint of personal data protection. However, in cases where opinions of the Office are not accepted, such as in relation to the intention of the Ministry of Health to implement the project of paper health cards, the Office must consistently perform control, as in the case of the joint project of the Ministry of Interior and the Ministry of Labour and Social Affairs concerned with certain problematic groups of youth.

In 2005, the Office was also requested by the Supreme State Attorney to provide collaboration in implementation of plans for transformation to electronic form of the files related to supervision by the state attorney over the activities of the Police.

Finally, it can be stated that, in 2005, the Office successfully continued to apply the principles of the right to protection of personal data on the basis of the high standards which it established in the previous years. Numerous responses to consultations and application activities even indicate that the Office is increasingly perceived as an institution protecting privacy in general, i.e. as an "Office for Protection of Privacy". Indeed, due to this perception of the position of the Office by certain parties submitting inquiries or requests for a standpoint, such persons are somehow frustrated in cases where the Office cannot exceed its statutory powers and, therefore, cannot provide assistance to the general public which turns to the Office with trust and in good faith.

VII. Inspectors of the Office – Findings from Controls Carried out in 2005

Control activities performed by the Office in 2005 included mainly ad hoc controls, i.e. examination of complaints; this fact was caused by the high number of requests for remedy and complaints delivered to the Office. A total of 80 ad hoc controls were carried out, of which 68 were completed. A total of 133 complaints were thus resolved. Certain complaints were handled by inspectors in a manner other than through control, i.e. by remedying the state of affairs. Controls were carried out in banks and leasing companies, business and construction firms, health-care facilities and pharmaceutical companies, and also in governmental agencies and self-governing bodies.

Several comprehensive controls were also performed on the basis of the control plan: of 13 control planned for 2005 and 7 that remained from the control plan of 2004, 12 were performed and completed, 2 were commenced, 2 were canceled, as the relevant institution had already been controlled on the basis of a complaint, and 4 were suspended. The controls were concerned with the police, prison service, banks, kindergartens, leasing companies, pharmaceutical companies, insurance companies, ministries, etc.

Within comprehensive control, inspections are aimed at all duties of the data controller, as imposed by the Personal Data Protection Act in processing of personal data, both in written and in electronic forms. The main areas of interest include the scope of collected personal data with respect to the purpose and statutory duties of the controller, possibilities of access by the data subjects to their personal data and fulfillment of the duty to destroy personal data after expiry for the period during which personal data need to be stored. With respect

to activities of governmental agencies, the purpose of personal data processing is based on the law and, therefore, the scope of processed personal data may not exceed the necessary extent corresponding to the statutory purpose. In relation to other controllers, the purpose follows from the contents of the agreement (written or oral) concluded with the data subject.

Amendment to the Personal Data Protection Act also imposed on inspectors the duty to ascertain whether the controller has drawn up documentation for securing personal data protection and whether he has duly informed the data subject of processing of his/her personal data.

A number of controls also encompass verification of the manner of processing of the birth numbers by reason that amendment to the Act on register of population and birth numbers of 2004 imposed much stricter requirements on processing of birth numbers; the supervision over compliance with that Act was entrusted to the Office.

During ad hoc controls, it is ascertained whether the relevant complaint is justified and whether the Personal Data Protection Act has actually been violated and whether the conduct in question constitutes infringement of rights of the complainant. It should be stated that, in some cases, an apparently simple ad hoc control based on a single complaint can turn out to be a very complex and time-consuming task, particularly in a situation where it is ascertained that, in fact, several instances of processing are involved or that personal data are being transferred by one controller to another. If it is established that personal data are not processed in accordance with the law, it is necessary to determine the core of the problem, i.e. whether and in what manner privacy of citizens has been endangered. Frequently, it is necessary to consult the relevant superior bodies and organizations in order to assess the need for processing of certain personal data.

Cases of violation of the law ascertained in 2005 were concerned especially with:

- unauthorized processing of inaccurate or excessive data;
- unauthorized transfer of data to another controller;
- insufficient or incorrect information of the data subjects;
- processing of sensitive data without express consent of the data subject;
- poor securing of personal data, e.g. as a consequence of unsuitable access rules in an information system allowing access to personal data also for unauthorized entities.

A total of 40 measures for a remedy were imposed; in 7 cases, administrative proceedings have already taken place and fines have been imposed.

Special attention must be paid to certain problems revealed during controls:

- Certain state administrative bodies or self-governing bodies are obliged to disclose certain information at request, e.g., to persons who have interest in a certain issue: for example, inhabitants of a city are entitled to inspect resolutions of the city council. However, this duty may not be fulfilled by posting information containing personal data on the internet; this step could result in unauthorized access to personal data (Article 13 of the Personal Data Protection Act) – indeed, through the internet, personal data are disclosed to an unlimited number of citizens, rather than only to authorized inhabitants of the given city.

- Personal data of third persons are also frequently processed without authorization; this occurs with respect to persons close to persons with whom the controller concluded a certain agreement (e.g. visitors of guests accommodated in a hotel) or persons whose personal data are legitimately collected by the controller (e.g. relatives of prisoners).
- Pursuant to Article 11 of the Personal Data Protection Act, *the controller shall be obliged to inform the data subject as to whom the personal data may be disclosed*. Thus, also in transfer of personal data for the purposes of direct marketing, the data subject should be informed of entities to which his/her personal data will be transferred (so that (s)he could disagree therewith, if appropriate). Companies often evade this duty by means of "general" consent to disclosure of personal data to other entities. However, the data subject must be informed before the data are disclosed (mere notification that personal data have already been disclosed contrary to the law). This duty was also often breached by banks within the provision of information on the annual percentage rate of costs (APRC) by telephone.
- When obtaining consent to transfer of banking information, the banks also often violated the law, particularly by combining and obscuring information on the purposes, scope and transfer of personal data of their clients in the general terms and conditions.
- Pursuant to Article 13 (2) of the amendment to the Personal Data Protection Act, the *controller shall be obliged to develop and to document the technical-organizational measures adopted and implemented to ensure the personal data protection*. This provision is neglected by many personal data controllers.

On July 29, 2004, the Chamber of Deputies of the Parliament of the Czech Republic approved Act No. 480/2004 Coll., on certain information society services and on the amendment to certain other acts (Certain Information Society Services Act), which entered into effect on September 7, 2004 after expiry of the required legislatively technical deadlines. It is necessary to reiterate that this Act is not a special law aimed against dissemination of "spam", but that it rather entrusted the Office with competence to punish cases of unsolicited commercial communications.

Although controls constitute the core of activities of the inspectors, their work is not completed by submission of the control protocol.

After completion of the control, it is necessary to notify the complainant as to whether violation of the law has been ascertained and in what manner remedy will be ensured on the basis of his/her complaint. In case of imposing remedial measures, a follow-up control is required to determine whether the measures have actually been adopted and whether the processing is in accordance with the law.

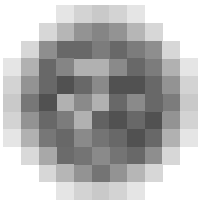
If inspectors establish during their control that a misdemeanour or administrative tort has been committed (Articles 44 and 45 of the Personal Data Protection Act), they submit the control results for proceedings on imposing a penalty.

In case of state administrative or self-governing bodies, it is often necessary to cooperate with the superior bodies of the controlled entity, because remedy can thus be ensured in an entire sector (e.g. education, social care, health care, etc.).

In 2005, the data controller subject to control could appeal against the control protocol to a senior inspector who was obliged to deal with his/her objections. If the controlled entity still was not satisfied with the solution, (s)he could refer the case to the President of the Office and, where liquidation of the processed personal data was ordered, also to the court.

Control activities often coincide with consultancy provided by inspectors. The controlled entities change the manners of processing of personal data, as they are often provided with new incentives and frequently consult their steps with the inspectors who performed control. E.g., upon introduction of a new information system, they request cooperation related to setting new security measures, i.e. they ask for assessment whether such measures are adequate from the viewpoint of personal data protection. The controllers often ask to whom they may or must transfer personal data, what processing and of which personal data is possible, e.g., in the framework of consent given by clients, etc. Thus, activities of the inspectors are not limited to performance of controls, but also include subsequent cooperation with the state administration and supervisory activities.

However, the basic objective of control is not to impose fines, but rather to ensure protection of personal data and privacy of citizens.



Foreign Relations and Participation of the Office in International Cooperation

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

The priority in development of foreign relations lies undoubtedly in cooperation with the European Union (the Commission), the Council of Europe and independent supervisory bodies for personal data protection in other EU countries, whose activities are governed by the same principles based on the "acquis communautaire" as the principles governing the activities of the Office. The basic legislation of the EU (EC) in the area of personal data protection that has been transposed to the legislations of all Member States includes 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 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, as well as Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

The most important working platform for relations and cooperation with both the European Commission and the partner supervisory bodies in other EU countries continued to be, in 2005, the Article 29 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 meetings involve high-level representatives of independent supervisory bodies, usually presidents of the relevant authorities. Its statements and opinions are intended particularly for the Commission and Committee 31 (see below) and have the character of recommendations; in addition, in its annual report submitted to the European Parliament and the Council, it can also address these EU bodies. Last but not least, documents drawn up by WP 29 are also very important for uniform interpretation of EU legal acts in the area of personal data protection, including particularly the aforementioned Directives, 95/46/EC and 2002/58/EC, and for harmonization of application approaches of the national supervisory bodies.

After accession of the Czech Republic to EU, a representative of the Office may participate, as a fully fledged member of the Working Group, in preparation of documents and standpoints with full power of his vote and thus affect the creation of EU policies in the given area. In 2005, a representative of the Office

(usually its President) participated in a total of eight meetings of WP 29, including the individual task forces. Important documents were discussed and adopted at these meetings, e.g., in the area of data protection in relation to intellectual property rights, radio frequency identification (RFID), Binding Corporate Rules of major supranational corporations, the Visa Information System (VIS), standards for security and biometric elements in travel documents, storage of operational data of service providers in public electronic communications for the needs of combating terrorism and serious crime, interpretation of Article 26(1) of Directive 95/46/EC on derogations in the transfer of personal data to third countries, and the Schengen Information System (SIS II). A number of other topical issues were also discussed, without adopting a final statement, e.g. in relation to processing of data of patients of health-care facilities, electronic health cards and enforcement of Directive 2002/58/EC (particularly in the area of spam, spyware, etc.).

The tasks of the secretariat with respect to the activities of WP 29 are ensured by the relevant organizational unit of the European Commission, "Unit C5 – Data Protection", which was transferred, at the beginning of 2005, from DG Internal Market to DG Justice, Freedom and Security, directed by Commissioner Franco Frattini. In addition to the WP 29 platform, an opportunity to pursue close relations and ensure joint addressing of issues together with experts of this body is also provided by participation in the meetings of the Committee for Personal Data Protection established by Article 31 of Directive 95/46/EC (hereinafter "Committee 31"), with which the European Commission consults all decisions and measures in the area of personal data protection, as a body providing for official representation of the Member States. If the adopted measures are not in accord with the standpoint of Committee 31, notice of this fact must be provided to the Council, which can then adopt a different decision. In 2005, a representative of the Office participated in two meetings of Committee 31. The third meeting planned for the end of 2005 was postponed due to the fact that a fundamental judgment of the European Court of Justice concerned with a transfer of personal data of air passengers from registration systems of airlines to the U.S. authorities is anticipated at the beginning of 2006. The main discussed topics included, e.g., preparation for similar measures in the area of transfer of data on air passengers, as agreed in relation to passenger air transport to U.S., and required also by Canada, Australia and New Zealand. Discussions are also concerned with adequacy of protection of personal data transferred from EU to U.S. on the basis of the agreed system of assertions on the part of U.S. companies and guaranteed by the U.S. authorities, designated as "Safe Harbor". The secretariat of the European Commission also provides this (rather political) advisory body with detailed information on the activities of WP 29, as a rather expert body.

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

Intersectoral cooperation between the Office and the bodies and working groups of the European Union, particularly in the framework of the Council/Coreper, continued with the same intensity. The Office also routinely cooperated with the Ministry of Informatics of the Czech Republic, particularly in the area of information society, electronic communications and e-Government. During the entire year, cooperation was pursued with the Ministry of Interior of the Czech Republic in relation to preparation of the European legislation on retention of data established in the use of electronic communications. In its posi-

tions, the Office strived to ensure that the relevant drafts are balanced and provide reasonable respect for the principles of protection of data and privacy.

Close cooperation with the Ministry of Interior of the Czech Republic, the coordinating body in the framework of the 3rd Pillar of EU, in relation to preparation for accession to the Schengen Convention, which presupposes creation of the National Schengen Information System (NSIS) with connection to the international Schengen Information System, continued in 2005. The Office attempts to create conditions necessary for the performance of supervisory powers in the area of processing of a major quantity of personal data entered into this system. These activities will include, not only supervision over the related national activities of the Police of the Czech Republic and other national bodies, but also fully fledged participation in activities of the Joint Supervisory Authority of Schengen (JSA), where the representatives of the Office are currently invited as observers. On the basis of accession to the Europol Convention, the authorized employees of the Office, as full members, already participate in the work of the Joint Supervisory Body of Europol (JSB) and, on the basis of accession to the Convention on the Use of Information Technology for Customs Purposes, also in the work of JSA Customs. Since December 20, 2004 (the 31st meeting of JSB Europol), inspector of the Office Mrs. Miroslava Matoušová has been discharging the office of vice-chairman of JSB Europol. In 2005, she was also involved in control performed in the Europol headquarters and in the work of two working groups; the Office also participated in the work of the Appeals Committee which deals with complaints of data subjects.

In 2005, the Office for Personal Data Protection paid increased attention to the subject of the Schengen cooperation and ***establishment of the Schengen Information System***, given the fact that the Czech Republic should accede to the Schengen area in 2007. However, this will be preceded by evaluations planned for 2006 and, therefore, the criteria of the Schengen acquis concerning personal data protection should be, in principle, fulfilled already in 2006.

Consequently, an informal working group headed by inspector Mr. Jan Zapletal has been established within the Office. It also includes two other employees of the Office (Mr. Jiří Maštalka, advisor of the President, and Mrs. Ludmila Nováková, lawyer active in the Department of Administrative Activities). These employees also participate in activities of the working group designated Schengen Evaluation – Czech Republic, established by the Ministry of Interior of the Czech Republic, particularly in activities of the expert subgroup for data protection, headed by Mr. Zapletal. In the framework of preparation for the evaluation, the Office for Personal Data Protection actively participated in the workshop "Preparation of the Czech Republic for the Schengen Evaluations", held on June 15 to 16, 2005. A meeting concerned with personal data protection within the Schengen Information System was held in the framework of the workshop at the seat of the Office.

Mr. Zapletal was also a member of an evaluation mission which took place in September 2005 in the Nordic countries (Nordics Evaluation - Data Protection, Reykjavik - Copenhagen, September 19 to 23, 2005). The task of the evaluation mission was to review the functions of the supervisory bodies of some countries involved in the Schengen Convention. The evaluation was concerned with the national supervisory bodies for personal data protection of Iceland, Norway, Denmark, Finland and Sweden.

This team, having a mandate of the Schengen evaluation working group and headed by Mr. David Smith of the Information Commissioner's Office of the United Kingdom, evaluated independency and powers of the national supervisory bodies for personal data protection and their control powers in relation to the National Schengen Information System (NSIS) and all bodies operating this sys-

tem or entering data to this system or withdrawing data from it. It also evaluated the safeguarding of NSIS against misuse of data and the possibility of the data subjects to access the information.

In 2005, representatives of the Office acted as observers in the framework of the Joint Supervisory Body for the Schengen Information System.

From the substantive viewpoint, the main attention in relation to the Schengen area was paid to the following aspects:

1. Ability of the Czech Republic to fulfill its obligations connected with supervision over personal data processing in the framework of the Schengen Information System.

2. Ability of the Czech Republic to ensure that, upon accession to the Schengen area, its legislation related to personal data processing will be in accord with the prescribed standards (Convention No. 108 and Recommendation of the Council of Europe (87) 15).

3. Ability of the Czech Republic to ensure that, upon accession to the Schengen area, personal data processing will actually take place in accordance with the aforementioned legislation.

In the framework of the thus defined topic, the following can be stated:

Re 1.
The independent Office for Personal Data Protection has been active in the Czech Republic since 2000 on the basis of Act No. 101/2000 Coll., on personal data protection; its competence includes supervision over all personal data processing, except for processing of personal data carried out by intelligence services. Everyone has the right to address the Office with a complaint or instigation concerning personal data processing. The conditions of Art. 114 of the Schengen Implementation Convention were thus fulfilled already In 2000.

In 2002, the activities of the Office were evaluated by an EU mission as corresponding to the EU standards.

The Office also annually performs a number of controls: some of these controls are concerned with activities of the Police of the Czech Republic which will act as a personal data controller also in relation to personal data processed in the Schengen Information System. Thus, it can be stated that, in this respect, the legislation of the Czech Republic is harmonized with the Schengen acquis.

A promotional campaign concerning personal data protection with respect to accession of the Czech Republic to the Schengen system should take place next year. The organizational background for the Schengen issues in the framework of the Office will also be strengthened.

Re 2.
From the viewpoint of the current legislation, the Czech Republic implemented Convention of the Council of Europe No. 108 of 1981 by adoption of Act No. 101/2000 Coll.

Recommendation of the Council of Europe (87) 15 was, in principle, transposed by the European amendment to the Police Act (Act No. 60/2001 Coll., amending Act No. 283/1991 Coll., on the Police of the Czech Republic, as amended).

Furthermore, from the legislative viewpoint, personal data processing is regulated particularly in the following laws:

– Act No. 326/1999 Coll., on the presence of foreigners in the territory of the Czech Republic and on amendment to some laws, as amended;

– Act No. 325/1999 Coll., on asylum, as amended;
– Act No. 13/1993 Coll., the Customs Act , as amended;
– Act No. 361/2000 Coll., on operation of vehicles on roadways, as amended;
– Act No. 56/2001 Coll., on the conditions for operation of vehicles on roadways, as amended.

The aforementioned laws are, in principle, mutually interconnected. Nevertheless, there are certain partial ambiguities and application issues whose solution might require adoption of, not only technical and organizational, but also legislative measures. Indeed, we consider it necessary that all procedures in personal data processing be properly and unambiguously stipulated directly in special laws, as only in that case is it possible to achieve full conformity with the Personal Data Protection Act, i.e. also with the Schengen acquis.

In near future, the Office will concentrate its supervisory activities on the above-described areas.

However, a note should be made of the existing interpretation ambiguities related to the potential for direct national application of the Schengen acquis upon accession of the Czech Republic, which must be eliminated as soon as possible, including any necessary measures to fulfill this requirement. The legislative group established by instruction of the Ministry of Interior of the Czech Republic No. 27/2005 has not reached any relevant conclusions to date. However, it can be reasonably expected that legislative changes will be made in the aforementioned laws.

Re 3.
With respect to the actual establishment of a national unit of the Schengen Information System, and the related provision for flow of personal data, activities of the Office for Personal Data Protection were strongly aimed at identification of any persisting ambiguities concerning, not only the creation of a technical background, but particularly responsibility for everyday operation and administration. In this relation, the Office clearly rejected certain persisting opinions, according to which it should bear certain responsibility for building this information system; it bases its negative viewpoint on the fact that this would be absolutely at variance with its supervisory mission. In any case, however, it is anticipated that certain steps and activities of the Office will need to be ensured in order to achieve conformity of the flow of personal data, particularly in the framework of the national unit of the Schengen Information System, with the legislation. Special attention in this respect will be paid to the aspect of fulfillment of duties pursuant to Article 13 of the Personal Data Protection Act, imposing the duty to physically secure the processed personal data. The Office will also pay attention to the area of filing and securing logs in order to ensure the possibility of tracing any potential abuse of the system for purposes other than those stipulated by the law.

Joint activities of representatives of supervisory bodies in the area of data protection from the countries of Central and Eastern Europe and Baltic countries, commenced in 2005 on the basis of an initiative of the Czech Office and the Polish Office of the General Inspector for Personal Data Protection, also continued in 2004. These activities have the form of working meetings (7th meeting of the Central and Eastern European Data Protection Commissioners, Smolenice, Slovak Republic, May 22 to 25, 2005) and other contacts, including communication with the use of common website (www.ceecprivacy.org). The final declaration adopted at this meeting stipulates the priority tasks for further cooperation of the aforementioned informal group of authorities in the CEE region.

From the viewpoint of bilateral relations with the partner supervisory bodies of other countries, the Office has established long-term above-standard cooperative relations with the Spanish Data Protection Agency (Agencia Española de Protección de Datos). An annual meeting with the employees of the Spanish Data Protection Agency took place on July 18 to 19 in Prague. The two-day program concentrated on three topical aspects: systems of electronic health documentation, use of biometric elements in passports and fight against spam. Experts from both institutions could share their opinions and latest experience. Together, they sought an answer to the question of how to ensure that the benefits brought by new technologies are not offset by infringement on privacy of individuals. With respect to spam, they examined what instruments are available to data protectors in detection and elimination of this unfavorable phenomenon. This interesting discussion was held in a friendly and informal atmosphere. Moreover, the meeting provided a welcomed opportunity to discuss topical details related to the forthcoming implementation of a joint twinning project in Bosnia and Herzegovina. Representatives of both parties drew up a memorandum of cooperation in which they committed to mutually cooperate in fulfillment of objectives of the project and specified important technical and economic aspects of their cooperation.

The Office also took advantage of the opportunity provided to Czech institutions by the Transition Facility. This instrument is defined in the Act of Accession (annex to the Treaty of Accession) as "temporary financial assistance to the new Member States to develop and strengthen their administrative capacity to implement and enforce Community legislation".

The project "Assistance to the Office for Personal Data Protection in Exercising Supervision in Personal Data Protection" will have the "twinning light" form. As its name indicates, the project will be concerned with strengthening and extending the knowledge and experience in supervisory activities. During eight months of its term, the project will particularly concentrate on two highly specialized areas: electronic communications and international police databases created in the framework of the Schengen cooperation, Europol and customs information systems. Attention will also be paid to employee data and protection of privacy at the workplace.

Austrian Ludwig Boltzmann Institute for Human Rights (Ludwig Boltzmann Institut für Menschenrechte) became the partner of the Office in implementation of the project on the basis of a selection procedure. The Austrian Data Protection Commission (Österreichische Datenschutzkommission) will support the aforementioned institute with respect to fulfillment of the goals of the project.

Negotiations on an agreement between the partner institutions took place in the autumn and the project will be implemented in 2006.

The Office also took part in the selection procedure for twinning project No. BA04-IB-OT-01 ***"Support to the Data Protection Commission of Bosnia and Herzegovina"***. This selection procedure was launched in the framework of the CARDS program, which is a program of the European Union to support stabilization of the situation in countries of the Western Balkan region.

The Office participated in the selection procedure as the senior partner, i.e. as the primary responsible institution, together with the Spanish Data Protection Agency, playing the role of the institution responsible for certain activities in the framework of the project.

The Office and its Spanish partner were successful in this selection procedure. The relevant contract was signed on November 3, 2005 in Sarajevo and on November 15, 2005 in Prague.

Thus, the Office became one of the first institutions in the Czech Republic to implement a similar project financed from the EU funds in a foreign country in the position of the senior partner.

The objective of the project is to improve the situation in Bosnia and Herzegovina (hereinafter "BiH") in the area of personal data protection with the objective of future integration of this country to the European Union. The project as such includes three main components:

1. Legal environment of BiH in the area of personal data protection
The main objective in this area will be particularly to revise the current Personal Data Protection Act of BiH, including its prepared amendment, in order to achieve conformity with 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. Furthermore, attention will be paid to personal data processing in the police sector, i.e. ensuring accordance with Recommendation R (87) 15 of the Council of Ministers to the Member States, providing for use of personal data in the police sector. Certain part of the relevant activities will concentrate on other sectoral legislation providing for personal data processing, e.g., in the area of public registers, banking, financial services, etc.

2. Functions of the Data Protection Commission of BiH
Activities will concentrate on creation of a model independent personal data protection authority capable of fulfilling tasks in accordance with the standards of the European Union. Such model authority must be, in particular, supported by the applicable legislation (see paragraph 1); however, it is also necessary to set up an internal organizational structure, effectively performing tasks in the area of supervisory, administrative and registration activities, foreign relations, etc. Direct training of the individual employees of the host authority is also anticipated in this respect.

3. Promotional campaign
The objective of these activities will be to raise awareness of the public in BiH in relation to personal data protection, which constitutes one of the pillars of successful work of a supervisory body. The activities will include a promotional campaign, provision of publicly accessible seminars and also events such as an open-door day.

In 2005, the Office participated in the work of 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; the former President of the Office, Mr. Karel Neuwirt acted as the vice-chairman of T-PD.

In the framework of OECD, in 2005, the Office continued to be involved in activities of the Working Party on Information Security and Privacy (WPISP) under the Committee for Information, Computer and Communications Policy (ICCP), in cooperation with the Ministry of Informatics of the Czech Republic, which is responsible for cooperation with OECD in the framework of activities of 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-regulative instruments in the given area, such as codes of conducts, alternative settlement of disputes, technology supporting privacy, etc. An important contribution of OECD in the area of competence of the Office can be perceived in the very sensitive and

topical seeking of 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. In this sense, OECD promotes the term "culture of security" connected with elaborated principles of the newly conceived Security Guidelines in the area of information. The topical issues assessed from the viewpoint of the culture of security include, e.g., the relation of information security and privacy to safety of traveling. Discussions also continued with respect to the long-term topic of new technologies and their impact on security and protection of privacy. A new topic consists in identity management.

The recent activities of OECD in the fight against spam are particularly important from the viewpoint of new competence of the Office in relation to unsolicited commercial communications. The employees of the Office (Ing. Jiří Krump, Ing. Antonín Šusta) became experts of the Task Force on Spam (TFS), which has prepared and gradually elaborates an Anti-spam Toolkit. Cooperation and joint activities of OECD/TFS and other organizations, such as APEC (Asia-Pacific Economic Cooperation) and ITU (International Telecommunication Union), are of special importance given the global nature of the subject of spam.

The following activities related to spam, involving representatives of the Office, should be mentioned:

- Fifth meeting of the national bodies dealing with strengthening of measures against unsolicited commercial communications – spam (Belgium, Brussels, April 6, 2005). The meeting of representatives of national authorities responsible for enforcing laws against unsolicited commercial communications was dedicated mainly to questions related to cooperation amongst the EU Member States in the fight against spam and issues related to disclosure of information necessary for the relevant investigation in individual cases.
- Sixth meeting of the national bodies dealing with strengthening of measures against unsolicited commercial communications – spam (Belgium, Brussels, July 7, 2005). The meeting was concerned primarily with the increasing use of "spyware" (Software that sends information about your Web surfing habits to its Web site.) and protection against it, including the possible technical and organizational measures on the part of providers of internet services.
- Meeting of the OECD Task Force on Spam and the related World Summit on the Information Society held by the International Telecommunication Union (ITU) – Thematic Meeting on Cybersecurity (Switzerland, Geneva, June 27 and 28, 2005). The OECD Task Force reviewed the state of preparedness of the Anti-spam Toolkit). The related meeting was concerned with the actual state of international protection against spam and stated that spam has moved to the sphere of organized crime and, therefore, it cannot be regulated, but rather only suppressed. The internet community will have to decide to what degree it wants the internet restricted and secured, or rather unrestricted and unsecured.

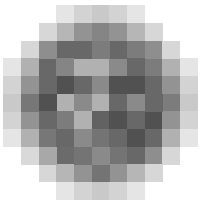
The foreign relations of the Office and the related participation in foreign meetings have been substantially developed also in relation to the new competence of the Office in the area of supervision in personal data protection, also for the reason of adoption of new obligations following, e.g., from the process of accession of the Czech Republic to the Schengen area. Participation in international events is also driven by efforts to respond to challenges following from modern information technologies.

Employees of the Office actively participated, e.g., in the following important events in 2005:

1. The ePSINet Policy Conference on Commercial Exploitation of Public Sector Information in Europe (Greece, Athens, January 14, 2005). The conference was concerned with the potential economic benefits following from further commercial exploitation of public sector information, the need to create a legal framework and national legislation, technical and organizational provision for access to information and creation of equal conditions for access to information.
2. Workshop "Czech-German Issues of Data Protection aimed at Transborder Data Flows" (FRG, Marktredwitz, January 20, 2005). The workshop was related to international and national legal aspects, practice and topical issues within the given subject. A major part of the workshop was dedicated to questions and instigations of the participants from amongst business entities.
3. Eleventh workshop on complaints handling (Hungary, Budapest, March 10 to 11, 2005). This regular workshop for employees of the personal data protection authorities concentrated on handling of complaints and the related administrative issues.
4. Spring Conference of European Data Protection Authorities (Poland, Krakow, April 25 to 26, 2005). The conference dealt with issues of harmonization of legislation in the EU countries, data protection in third countries, implementation of Directive 95/46/EC, enforcement of data subjects' rights, education and awareness raising on data protection. Furthermore, it also addressed the need for improved exchange of information, including personal data, between law enforcement bodies of EU and similar authorities of third countries in relation to terrorism and serious crime. However, it also emphasized the need for adherence to the principles of protection of fundamental human rights and freedoms. Certain principles for implementing regulations in this area were formulated.
5. 7th meeting of the Central and Eastern European Data Protection Commissioners (Slovakia, Smolenice, May 22 to 25, 2005) This regular event was concerned with the subject of processing biometric data, personal data for statistical purposes and data in the area of health care and justice. The participants also dealt with questions of securing data in information systems and disseminating knowledge on personal data protection.
6. Modern state administration between freedom of information and data protection (Germany, Schwerin, June 1, 2005). The right to information (freedom of information), on the one hand, and the right to personal data protection, on the other hand, are in apparent contradiction. Indeed, a majority of presentations made at this workshop were concerned with examination of this fact.
7. Summer academy "Service through a mouse-click – e-Government respecting data protection" (FRG, Kiel, August 29, 2005). The conference indicated that electronic communication is becoming a matter of fact and that future belongs to this phenomenon. It also pointed out that the current state of affairs in the area of protection of identity and management thereof is unsatisfactory and indicated the direction of its further development.
8. European workshop concerning standards for ensuring confidentiality in relation to patients and their privacy during health care (Belgium, Brussels, September 8, 2005). The objective of the workshop was to acquaint the participants with approaches and opinions concerning standards for disclosure of information on health care of patients by entities managing such data.
9. 27th International Conference of Data Protection and Privacy Commissioners (Switzerland, Montreaux, September 14 to 16, 2005). The motto of the conference was "Protection of personal data and privacy in the globalized world:

Universal right respecting differences". This also became the main subject of this meeting of presidents of accredited bodies for personal data protection ("commissioners") accompanied by selected senior employees and with participation of invited experts and representatives of international organizations active in the given area.

10. International symposium "Freedom of Information in Germany and Europe" (FRG, Postupim, September 28 to 29, 2005). Presentations and discussion of the participants were concerned with the apparently antagonistic relation between freedom of information and the right to data protection. It was stated that these two categories could exist along each other and that the necessary balance must always be sought. Freedom of information is a necessary precondition for functioning of a democratic society, as is the right to privacy and data protection.
11. Twelfth workshop on complaints handling (France, Paris, November 17 to 18, 2005). This regular workshop for employees of the personal data protection authorities concentrated on handling of complaints and the related issues.
12. International Scientific Conference on Data Protection in Law Enforcement – "Freedom, Security and Justice".



The Office, Media and Means of Communication

After five years of its existence, the Office has created a manner of communication that could be characterized as "Always and Faithfully": it is always ready to answer questions raised by journalists, often representing the public, and deal with cases revealed by the media. It is faithful to the tradition of regular quarterly meetings with journalists and to the established character of the thus-planned press conferences which balance the previous periods. It thus primarily raises awareness of the public of 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. The effort to be as open towards the public as possible is also expressed in the fact that each quarterly press conference, inter alia, provides information on both the contents and scope of work carried out by the Office in the given period.

With respect to the previous year, it can be stated that the questions addressed to the Office by journalists reflect great trust in credibility and expertise of this institution. The questions frequently knowingly exceed the scope of competence of the Office and the inquiring persons introduce their requests by the words "If you could give me advice…".

Understanding that legal issues usually cannot be dealt with by immediate statement that the law has or has not been violated is also apparently increasing. However, this does not mean that, during the previous year, the Office did not encounter any striking simplifications of its explanations, that it did not find quotations put in "quotation marks" without such words ever being said, or that its statements were not subject to false interpretation and manipulations on the basis of an opinion which the relevant party strived to enforce a priori. While these cases are relatively seldom, nevertheless, we must be aware of them in the interest of the public.

As stated in the previous report, the number of articles in the media substantially increases after each press conference. They also reflect the interests of individual media, their profile and character of their readers. Thus, the Office has a welcomed opportunity to reflect problems that it considers substantial from the professional viewpoint, compared to priorities selected by the media.

PRESS CONFERENCES

Two press conferences held last year were absolutely unique – they were dedicated to extraordinarily important events: the summer conference (June 15, 2005) reviewed the five years of existence of the Office.

In September, the press conference was concerned especially with the new President of the Office and his strategic decisions and plans.

Facts related to the work of the individual components of the Office, statistical surveys of commented laws and other legislation and surveys of sanctions 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.

The press conference, which took place in December 2005, traditionally balanced the quarterly work; however, information was also provided on the initial implementation of the first of the plans of the new President – extending the scope of discussions amongst both the professional and lay public. Through the website, the public could learn the principles of use of camera surveillance systems, which were drawn up by the Office both as legal interpretation from the viewpoint of the Personal Data Protection Act and as a basis for application of the given Act in that area. A public commentary procedure of its sort takes place within the discussion forum. After evaluation of the opinions and suggestions following from this discussion, a fundamental recommendation will be drawn up with respect to the use of camera surveillance systems that is not at variance with the Personal Data Protection Act. The Office accepted comments from December 19, 2005 to January 15, 2006.

An important part of every press conference is dedicated to a certain segment of work of the Office: e.g., at the meeting with journalists in December, this analysis was concerned with activities and representation of the Office in control and supervisory bodies of EUROPOL and the Schengen Information System.

The response of the media to the press conferences is very clear: on average, 5 to 7 articles in the monitored Czech media deal with personal data protection every day, while, during the first three days after each press conference, the number of such articles increases to approx. 15 to 35.

PUBLISHING ACTIVITY – DISSEMINATION OF NEW EUROPEAN AND GLOBAL FINDINGS

In 2005, the Office issued four editions of the Journal. Although the number of issued editions was lower compared to previous years, this can be explained by the fact that the last amendment to the Personal Data Protection Act canceled the duty of the Office to publish in a printed form a survey of newly registered cases of processing within two months of registration. Currently, only canceled registrations are published in a printed form.

However, on the other hand, the sections of the Journal containing 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 translated either at own instigation of the Office or are directly adopted from the Official Journal of EU, have become more extensive.

The bulletin of the Office, which is intended for a wider public than the Journal oriented on the professional public, aims at raising awareness of personal data protection and provision of information on the most important global events concerning protection of privacy; simultaneously, it provides a periodical survey of activities performed by the Office during the previous quarter or a similar period. The latter part of the bulletin reflects the efforts of the Office to be as open and transparent for the citizens as possible. An informative article dealing with

the phenomenon called "phishing" was the most interesting material of 2005. In fact, this phenomenon caught attention of the entire range of Czech periodicals which dealt with it by reference to the bulletin of the Office (20 articles were published in daily papers alone).

OTHER MEANS OF COMMUNICATION

The website of the Office, which has been positively evaluated as regards the scope of provided information, underwent a change of the graphic design in 2005. Its introduction is planned in the first quarter of 2006. The website will also contain several new sections – primarily sections providing information which must be published under law (e.g. the Official Board), as well as those that improve the contacts and relations with the public (e.g. the sections reserved for consultancy, advice for parents and children, etc.) or that increase the openness and transparency of activities of the Office for the public and strengthen public contacts (the more extensive section describing the structure of the Office, access to information on the budget, information on jobs offered by the Office, more extensive use of the discussion forum for provision of public comments on documents of the Office) and, last but not least, the continuous and direct access to information on the current work of the Office. Emphasis in the creation of the website was also placed on user comfort. This includes, e.g., the possibility of electronic filing of the registration form or accessibility of the website for health-impaired citizens.

In 2005, the Office also distributed 200 000 information leaflets on personal data protection to the self-governing bodies – from city councils to municipal boards; in total to 6 370 places. In the accompanying letter, the President addressed the representatives of the self-governing bodies with request that they enable, according to local customs, access of the citizens within their jurisdiction to the leaflet and to information formulated with respect to raising awareness of the citizens of the right to protection of privacy.

In a number of cases, the self-governing authorities subsequently requested that the Office provide them with information in electronic form for their own websites, or with a request for publication of information contained in the leaflet in a form required for the needs of their own periodicals, e.g. continual text of articles, etc.

Additional 100 000 leaflets were later acquired. These leaflets were intended to satisfy any additional requirements of self-governing bodies and primarily, they were distributed on the basis of cooperation with the Ministry of Education, Youth and Sports (within information provided by the Ministry) to regional school authorities, with request that the leaflet be used at secondary comprehensive schools. In relation to this activity, the Office also took advantage of the opportunity provided by that Ministry to meet representatives of regional school authorities. In the framework of the meeting held in Zlín, with participation of the President and the spokesperson of the Office, representatives of the school authorities were informed of the subject of personal data protection and they were offered the information leaflet. In this case, the leaflet was distributed on the basis of requirements of the regions. In relation to the aforementioned meeting in Zlín, a meeting was also organized for the headmasters of secondary schools in Liberec.

5 000 leaflets were distributed through journal Moderní obec (Modern Town).

In all parts of the information campaign, the Office strived not to create the impression of any pressure being exerted by it, but rather that it be clear that it

respected the various local customs, which are better known by the local government, and that it provide service to the citizens.

Such communication with the general public is also planned for the next year – inter alia, with emphasis of information about personal data protection in the Schengen area.

BENY TV company together with the Czech Television has provided the Office in 2005 for non-commercial use with a part of its series "Ignorance is not an excuse", concerned with personal data processing.

In the framework of communication and public relations, the Office also provided, in the framework of a twinning project, support to the supervisory authority of Bosnia and Herzegovina; more detailed information on this project is contained in the chapter dedicated to foreign activities and relations of the Office (see p. 43). The project shall be realized during 2006.

LIBRARY AS A PROFESSIONAL BACKGROUND

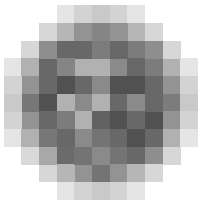
The professional library of the Office which provides a background for its own employees, served last year also to students of secondary schools and universities who dealt with personal data protection in their seminary, final and diploma theses (6). A majority of work created with support of the library of the Office subsequently becomes part of the library, whereby a unique library fund is created in the Czech Republic.

The Office also supports experts who will, in turn, help to raise awareness, improve knowledge of personal data protection, as well as the respect for personal data protection – the key to privacy of each citizen.

COMMUNICATION OF THE OFFICE WITH MEDIA IN FIGURES:

Period: January – December 2005

Agency service	18
Total press	177
Of which:	
Daily press	125
Other periodicals	52
Television	52
Radio	27
Total media	**274**



Administration and Development of the Information System

The information system was developed in 2005 particularly by the following means:

1. Renewal of hardware
2. Modernization of active elements and the basic cable network
3. Upgrade of Microsoft Windows software products for servers and workstations
4. Upgrade of the website of the Office
5. Development of applications to support control and administrative activities
6. Creation of a safe remote connection to the information system of the Office

Renewal of hardware included full replacement of servers of the Office and of the backup library, and installation of a single data space. In this relation, both active and passive parts of the network were subjected to modernization, with the objective to improve their reliability and speed.

Upgrade of Microsoft Windows software products for servers and workstations is carried out by means of the license model for these products – the multi-license "Microsoft Enterprise Agreement". The basic conditions for standardization of the software equipment were thus created, enabling to plan expenditures for upgrade of software products sufficiently in advance. Development of an application to support the basic activities of the Office continued in 2005, including, e.g. modification of the module for addressing complaints against unsolicited commercial communications, development of a module for control and administrative activities and preparation of a new version of the module for registration of personal data controllers.

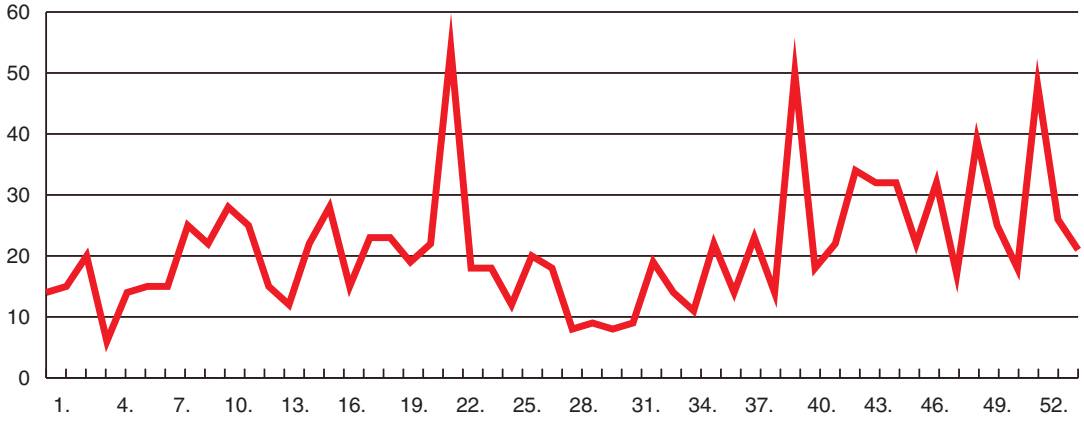
A fundamental upgrade of the filing service was carried out. The program applications used by the Office were gradually modified, both from the viewpoint of new functions related to legislative changes and from the viewpoint of a new version and comprehensive introduction of the filing service.

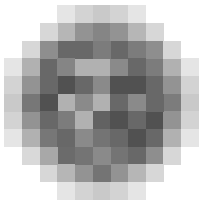
Considerable efforts were exerted to improve the protection against unfavorable penetration into the system and attack of viruses. An information security management study was drawn up. This study included analysis of IS risks and in-depth security tests. This enabled to set the security plan of the Office as the basic document for stipulating the strategy of data protection and the information system and issue of the relevant regulations. Furthermore, a new antispam protection module for the information system, including improved heuristic analysis, was introduced during the year.

UNSOLICITED COMMERCIAL COMMUNICATIONS

Act No. 480/2004 Coll., on certain information society services and on the amendment to certain other acts, entrusts the Office with a new area of competence in the field of supervision and assessment of unsolicited commercial communications circulated through electronic means. In 2005, the Office received a total of 1105 instigations related to sending unsolicited commercial communications (UCC). A survey is provided in the following chart.

Number of received instigations related to sending UCC in 2005





Personnel of the Office

As of December 31, 2004, the Office for Personal Data Protection had 74 employees; for 2005, the state budget set the number of personnel at 77.

Mr. Igor Němec was appointed by the President of the Czech Republic, based on nomination by the Senate of the Parliament of the Czech Republic, to the office of President of the Office for Personal Data Protection for a term of five years from September 1, 2005. Work continued under his direction with respect to optimization of procedures in the performance of administrative activities which were commenced in 2004 by establishment of the new organizational department – Section of Control and Administrative Activities of the Office. The objective of the contemplated organizational changes is to create an organizational structure of the Office that will ensure the necessary services for inspectors of the Office and, thus, maximum effectiveness in the performance of control and administrative activities 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).

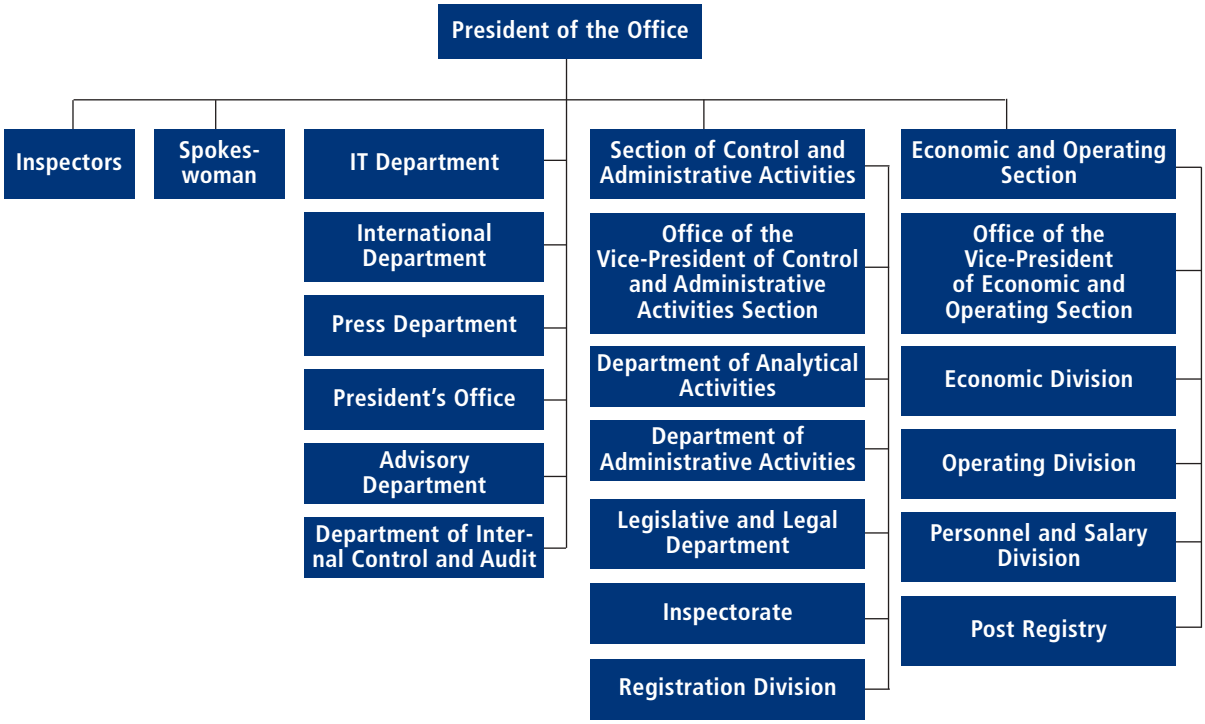
Classification of employees of OPDP according to age and sex – as of December 31, 2005

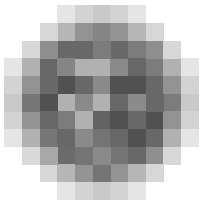
Age	men	women	total	%
21 to 30 let	2	9	11	13,75 %
31 to 40 let	5	4	9	11,25 %
41 to 50 let	8	10	18	22,50 %
51 to 60 let	23	14	37	46,25 %
61 and older	4	1	5	6,25 %
Total	42	38	80	100 %
%	52,50 %	47,50 %	100 %	

Classification of employees of OPDP according to education and sex – as of December 31, 2005

Education	men	women	total	%
University	34	14	48	60,00 %
Higher vocational	0	1	1	1,25 %
Complete secondary vocational	4	18	22	27,50 %
Complete secondary general	2	4	6	7,50 %
Secondary vocational	1	1	2	2,50 %
Vocational training	1	0	1	1,25 %
Total	42	38	80	100 %

Organizational structure of the Office for Personal Data Protection





Economic Management of the Office

The budget of the Office was approved by Act No. 675/2004 Coll., on the state budget of the Czech Republic for 2005.

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	41 052,29
Total expenditures	71 051,67

Individual expenditure indicators

General individual indicators:

Salaries of employees and other payments for performed work	28 841,79
of which: salaries of employees	28 294,45
other payments for performed work	547,34
Mandatory insurance premiums paid by the employer *)	10 100,78
Contribution to the Cultural and Social Needs Fund	565,61
Expenditures for financing programs pursuant to Schedule No. 5	20 119,48
of which: capital expenditures	8 323,89
non-investment expenditures monitored in ISPROFIN	11 795,59
Common non-investment expenditures and related expenditures	21 003,82
Transfer to the reserve fund	2 420,00

Specific individual indicators

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

Income

Income was not classified within the budget for 2005. The total income of Chapter 343 - Office for Personal Data Protection equaled CZK 41 052,29 thous.

This income consisted particularly of refunds for foreign trips of employees of the Office from the Council of Europe and the European Commission, interest on money deposited in accounts kept by the Czech National Bank, an insurance benefit, transfers from own funds and income related to 2004 (transfer of the balance of the deposit account after payment of salaries and the allocation to the Cultural and Social Needs Fund for December 2004).

The income account included the use of money from the reserve fund in a total amount of CZK 813,30 thous. for the supplementation of the mobile equipment on the premises of the Office. Furthermore, the amount of CZK 260 thousand from the reserve fund was used for refundment of costs of „Electronic filling department“ action.

Interest on money deposited in accounts kept by the Czech National Bank equaled CZK 165,81 thousand.

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

1. Common expenditures

Withdrawals for common expenditures in an amount of CZK 21 003,82 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 899,37 thousand in 2005.

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 (see the Table).

As of December 31, 2005, the personnel consisted of 80 employees.

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

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

A total of CZK 20 119,48 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 8 323,89 thousand were used for investment expenditures. 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 of ICT OPDP", where *systemic investment expenditures from the state budget* were incurred in 2005 for:

	in CZK thousand
project 243011 0002 "Extension of the IS program"	662,53
project 243011 0007 "Reproduction of computer networks"	586,86
project 243011 0009 "Electronic filing department – filing service"	701,53
project 243011 0010 "Renewal of servers"	3 133,96
project 243011 0011 "Acquisition of a notebook"	81,99
project 243011 0013 "Acquisition of notebooks"	116,23
project 243011 0014 "Upgrade of Microsoft servers and the OS of workstations"	776,33

systemic non-investment expenditures from the state budget for:

project 24301P200 "Operation of ICT of the Office"	6 747,76

Subprogram 243 012 "Reproduction of OPDP assets"

– where *systemic investment expenditures from the state budget were* incurred in 2005 for

project 243012 0111 “Construction repairs of the administrative building” 488,92
project 243012 0116 “Acquisition of a kitchen unit” 80,76
project 243012 0118 “Acquisition of a high-capacity vehicle (microbus)” 809,29
project 243012 0119 “Acquisition of multifunctional copying machines” 665,50

systemic non-investment expenditures from the state budget for:
project 243012 5501 “Rent and services” 2 587,05
project 243012 5502 “Maintenance of equipment and long-term investment assets” 1 647,47
project 243012 5503 “Provision of mobile equipment for offices” 813,30
(means for this fund were withdrawn from the reserve fund)

Non-investment systemic expenditures were withdrawn in an amount of CZK 11 795,59 thousand 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

In accordance with the adopted plan, Český a moravský účetní dvůr s.r.o, carried out an audit aimed at public procurement. The findings will be incorporated in an internal directive. Other external audits were postponed to 2006 due to the pending fundamental organizational and personnel changes.

At the present time, the internal audit function lacks personnel and the Office plans to deal with this issue through external contractors.

5. Use of the reserve fund

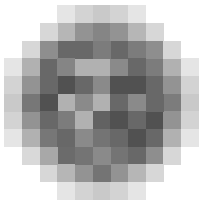
Part of the means in the reserve fund were used to finance subprogram 243012 5503 “Provision of mobile equipment for offices”, in an amount of CZK 813,30 thousand and CZK 260 thousand to finance "Electronic filing department" action.

Survey of use of the budget in 2005

Budgetary item	Name of indicator	Approved budget for 2005 in thous. CZK	Modified budget for 2005 in thous. CZK	Actual facts pursuant the accounting records as of December 31, 2005 in thous. CZK	Fact / modif. budget in %
	Total income	**0**	**0**	**41 052,29**	**0**
501	Salaries	27 066	28 316,00	28 294,45	99,92
5011	Salaries of employees	20 111	20 111,00	20 104,09	99,97
5014	Salaries of employees derived from salaries of constitutional officials	6 955	8 205,00	8 190,36	99,82
502	Other payments for performed work	1 990	1 740,00	547,34	31,46
5021	Other personal expenditure	1 109	859,00	547,34	63,72

5024	Compensation	300	300,00	0,00	0,00
5026	Severance pay	581	581,00	0,00	0,00
503	Mandatory insurance premiums paid by the employer	10 170	10 520,00	10 100,78	96,02
5031	Mandatory premiums for social security	7 555	7 815,00	7 509,54	96,09
5032	Mandatory premiums for public health insurance	2 615	2 705,00	2 591,24	95,79
513	Purchase of materials	8 250	8 415,00	3 421,35	40,66
514	Interest and other financial expenditure	20	20,00	14,02	70,10
515	Purchase of water, fuels and energy	1 350	1 350,00	1 119,93	82,96
516	Purchase of servuces	24 486	22 836,00	10 441,56	45,72
5167	Training and education	1 000	1 000,00	788,14	78,81
517	Other purchases	8 113	8 222,00	4 160,95	50,61
5171	Repairs and maintenance	4 893	4 692,00	1 272,84	27,13
5173	Travel allowances	2 450	2 300,00	2 020,31	87,84
518	Advance payments provided	0	1,00	-0,11	-11,00
519	Expenditures related with non-investment purchases	2 269	2 269,00	1 846,12	81,36
534	Transfers to own funds	541	566,00	2 765,61	488,62
5342	Transfers to the Social and Cultural Needs Funds	541	566,00	565,61	99,93
536	Other non-investment transfers to public budgets	10	10,00	5,60	56,00
542	Compensation to citizens	60	60,00	10,18	16,97
5429	Other compensation to citizens	60	60,00	10,18	16,97
	TOTAL CURRENT EXPENDITURES	84 325	84 325,00	62,727,78	74,39
611	Acquisition of long-term intangible assets	401	2 070,00	2 294,12	110,83
612	Acquisition of long-term tangible assets	7 665	5 996,00	5 809,77	96,89
6361	Investments transfer to reserve fund			220,00	
	TOTAL CAPITAL EXPENDITURES	8 066	8 066,00	8 323,89	103,20
	Total expenditures	**92 391**	**92 391,00**	**71 051,67**	**76,90**
	of which: use of the reserve fund			1 073,30	

The figures were adopted from statements drawn up as of January 31, 2006.



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

Re: Article 18 (1) (a)

In 2005, the Office received 12 inquiries qualified by the inquiring parties as request for information pursuant to Act No. 106/1999 Coll.
However, all inquiries were dealt with by reference or advice of their correct qualification.

Re: Article 18 (1) (b)

During 2005, the Office received 5 inquiries pursuant to the Act on Free Access to Information.
In 6 other cases, the inquiries concerned consultations with clarification of duties imposed by Act No. 101/2000 Coll., on personal data protection, as amended.
Another inquiry concerned Act No. 480/2004 Coll., on certain information society services.
Of the 6 inquiries related to the consultation duty imposed on the Office by the Personal Data Protection Act, one case involved a justified complaint which was dealt with by the Office within its control activities in accordance with its duty of a supervisory body.
However, in all cases, the Office answered the inquiries within the deadlines stipulated by Act No. 106/1999 Coll., on free access to information.

Re: Article 18 (1) (c)

Not applicable in 2005.

Re: Article 18 (1) (d)

No proceedings held or penalties imposed.

Re: Article 18 (1) (e)

Not applicable in 2005.