the office
for personal
data protection

ANNUAL REPORT SUMMARY 2008

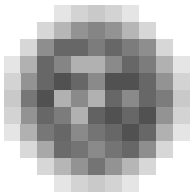
Year 2008 from the Viewpoint of the President of the Office

When looking back at the year 2008, I cannot see any radical change in the trend of preferring collective security to the right to privacy, which I noted at the end of 2007. However, the Office for Personal Data Protection cannot and does not intend to play a passive role of a mere observer of the mentioned trend. This is documented by the present Annual Report. However, it provides not only a detailed summary of the work carried out last year. It also illustrates the efforts of the Office aimed to improve care for privacy of citizens already in the phase of preparation of legal rules that will affect their fundamental right to protection of private life. I am glad to note a certain improvement in personal data protection within the Land Registry. While the state of affairs is far from ideal, compared to the original uncontrollable use of this database, which substantially affected the lives of thousands of citizens, it is now possible to immediately respond to suspicious utilisation of data and, where unlawfulness of such action is proven, to impose the consequent punishment. I also state with satisfaction that the Office has embarked on a route, which certainly will not be easy, of seeking rules for responsible treatment of genetic data. The state of affairs that we have ascertained gives no reason for light-hearted optimism, but we are now aware of the need to closely focus on processing of data in DNA databases. Indeed, these data are the most sensitive and their misuse could have fatal consequences also for future generations. We have also obtained a number of important findings related to the use of camera surveillance systems. However, I must regret that the ensuing proposals to the legislature, which could have improved the situation in the use of camera surveillance systems by the Police of the Czech Republic, have been trapped in the negotiating process. The absurd utilisation of this highly intrusive means is also documented in this Annual Report in the form of a pictorial annex. Unfortunately, the smiles it causes quickly become sour and this whole issue lies beyond comprehension … It must also be noted that this year's Annual Report more than ever provides not only a summary, but also a number of specific findings, both for the general public and the legislature and executive bodies. In the part concerned with control activities, we focused on several areas – information systems of the public administration, health care, information systems in the area of justice and State attorney's offices, personal data protection and the aspects of DNA, information systems of the EU, the RFID technology, particularly in relation to chip cards in transport – and we thus collected numerous interesting materials. A detailed description of the individual cases, the procedure in administrative proceedings as well as second-instance proceedings, and the judicial review, provides a thorough insight in the process of control itself, as well as in the issues revealed by the control; these are de facto model examples that could provide guidance for both personal data controllers and administrative agencies in decision-making on personal data processing. We thus also offer findings on personal data protection as an increasingly important part of human rights. A similar benefit should ensue from the extensive chapter of the Annual Report concentrating on supervisory activities and on the topics which are dealt with by the relevant organizational unit of the Office. Clear satisfaction can be drawn from the results of the Office's international activities. It can be stated that the Office is being perceived abroad as a credi-

ble and beneficial partner. This justifies my conviction that it will also successfully deal with all the tasks that it will face during the Czech Presidency of the EU Council. And there will be many. The worth of our efforts to provide information to the citizens is also clearly confirmed by the fact that the Office's website has been selected and included amongst those information sources that will be retained for the future as national heritage. Whereas the global conference of personal data protection commissioners that was held in Strasbourg in October 2008 paid great attention to the issue of youth and new technologies and placed emphasis on the need for dissemination of knowledge on personal data protection amongst the young generation, it should be noted that the Czech Office has already been intensively working with youth and teachers for two years. A project accredited by the Ministry of Education, Youth and Sports of the Czech Republic concentrating on ongoing education of teachers is now entering its third year and has drawn real interest and positive evaluation on their part. Our annual meeting with young people on the occasion of the competition "My privacy! Don't look, donęt poke about!" is a pleasure for us. The Office thus presents its Annual Report with a feeling of accomplishment after a year of intensive work. Similar intensity will undoubtedly be required in the next half year marked by the Czech Presidency of the EU and the Office will also be preparing for the european privacy and data protection commissionersę conference, to which it will have to invite its partners as early as in the spring of 2009. However, I have faith in the people who I work with and, therefore, I have absolutely no doubt that both the major one-off tasks which we will face in the near future and the long-term every-day work will fulfil the mission of the Office: to protect personal data and to serve for protection of the fundamental human right to private and family life.

Igor Němec

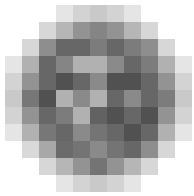
Contents



Office in numbers – 2008

inquiries and consultations	inquiries in the Czech Republic	1 813
	abroad	130
	personal consultations total	115
	for State administration	35
	for local governments	17
	for legal persons	46
	for natural persons operating a business	10
	for natural persons	7
Instigations and complaints	instigations received pursuant to the Personal Data Protection Act	697
	complaints referred for control	202
Unsolicited commercial communications (competence pursuant to Act No. 480/2004 Coll.)	total instigations	1 458
	instigations resolved	1 311
	controls initiated	155
	controls completed	91
	administrative decisions on a fine	81
Controls (excluding controls concerning Act No. 480/2004 Coll.)	initiated	112
	completed	112
	referred to other governmental authorities	45
	challenged by objections	35
	objections accepted	12
	objections dismissed	14
	mostly accepted	1
	mostly dismissed	3
Administrative punishment	administrative proceedings for violation of Act No. 101/2000 Coll. and No. 133/2000 Coll.	87
	misdemeanour proceedings pursuant to Act No. 101/2000 Coll.	8
	misdemeanour proceedings for violation of Act No. 159/2006 Coll., on conflict of interests	0
	appealed decisions on violation of law	33
	appeals dismissed	16
	cancelled and returned for new hearing	1

	cancelled decisions and proceedings discontinued	2
	change in the decision	2
Judicial review	court actions lodged	13
	actions dismissed by the court	1
	decisions cancelled by the court	0
	court proceedings closed / pending	1/12
Registration	notifications received (pursuant to Article 16 of Act No. 101/2000 Coll.)	3 327
	instances of processing registered	2 841
	controllers registered	1 914
	registrations cancelled	90
	notifications on a change in the processing	1 141
	proceedings pursuant to Article 17	99
	discontinued (no violation)	78
	discontinued for procedural reasons (e.g. notifications withdrawn)	9
	not permitted	12
Authorizations for transfers of personal data abroad	applications for transfer of personal data abroad received (pursuant to Article 27 of Act No. 101/2000 Coll.)	23
	decisions on authorization of transfers	33
	decisions on dismissal	0
	proceedings discontinued for procedural reasons	6
Complaints pursuant to Article 175 of the Code of Administrative Procedure	complaints received	33
	decisions on dismissal	6
	complaints found partly justified	5
	complaints found unjustified	24
Complaints and other instigations related to the procedure of the Office that were not resolved pursuant to Article 175 of the Code of Administrative Procedure	instigations received	1
	instigations found justified	1
	instigations found unjustified	0
Applications pursuant to Act No. 106/1999 Coll.	applications received	6
	applications resolved	6
	applications refused	0
Materials published	Journal of the Office (number of volumes)	3
	Bulletin of the Office (number of volumes)	4
Press conferences	regular press conferences	4
	extraordinary	1
Commented legislative drafts	laws	69
	implementing regulations	48
	other	80



Control activities

General aspects of control activities

Almost 90 % of controls were carried out on the basis of instigations and complaints in 2008; the remaining controls took place according to the control plan. Complaints for violation of Act No. 480/2004 Coll., on certain services of the information society, concerning the sending of unsolicited commercial communications, were mostly lodged via the Office's web form. Instigations that are dealt with by inspectors can be divided into two basic groups – complaints for one-off violation of the law and complaints indicating a suspicion of systemic violation of the law. In one-off controls, the given issue is often dealt with and resolved already within "preliminary investigation procedures". In these cases, remedy is ensured without formal control. While this procedural institute is not explicitly stipulated in the Act, it can nevertheless be deemed to fall within the competence of the Office pursuant to Article 29 (1) (a) of the Personal Data Protection Act and it follows from the Office's duty to perform supervision of compliance with the duties stipulated by the law. This procedure cannot be employed in all cases and in respect of every controller. However, once this method is chosen, it has been found that a majority of representatives of the given entities cooperate with the inspectors. This attests, e.g., to the increasing informal authority of the Office. A positive role could also be played by the Office's consultation duty. This procedure is applied in cases where misconduct is not intentional. We are thus referring to a form of supervision which guarantees that the case is closed within a short term. A similar procedure is also used in resolving the rare complaints for violation of the Act on Certain Services of the Information Society, where the Office would proceed uneconomically if it were to attempt to find the author of a single e-mail message. Nevertheless, a vast majority of cases are still being resolved by inspectors within the performance of ordinary state control. Within controls of major entities – regardless of whether these are governmental authorities or large private corporations – the control workers usually encounter professionally skilled and experienced persons who are aware of and enforce the rights of the controlled entity and, in most cases, have a good legal background. In contrast, in small, predominantly private entities, the inspectors continue to encounter, during control meetings, minimum legal awareness of the duties in the area of personal data protection, which is, in some cases, masked by arrogance against the controlling persons. In these cases, it is more frequently necessary to refer to enforcement means stipulated by law, which allow for attainment of the control objective. More frequently than in the previous years, the performed controls indicated that certain complainants take advantage of the competence of the Office for Personal Data Protection, being aware that the law requires that it investigate every instigation. However, it is often found, during the control, that the person who sent the instigation had been, e.g., recorded by a camera and his or her unlawful conduct proven on the basis of the recording. It is striking that such instigations are often lodged by lawyers on behalf of these persons. Increasingly often, the Office is being misused in disputes amongst various entities, where the fact that personal data processing is reflected in almost all ac-

tivities is being abused as a "by-product" in the dispute. These mala fide instigations and complaints burden the control activities and waste time required for justified cases, where control is really required. The year 2008 can also be characterized, in the field of control activities of the Office, by the fact that remedies are being more frequently used to challenge control protocols, which fact can be attributed to the increasing qualifications of the controlled persons. Nevertheless, it can be stated that the fraction of control findings that were cancelled by the second-instance body did not increase compared to the previous years.

Control activities according to the control plan

As stated above, the **performance of control activities** of the Office is not determined only by the area at which complaints or instigations are aimed at a given time; the Office pursues a number of its control activities on the basis of a control plan which is approved and evaluated by the President of the Office together with the inspectors every year. In 2008, the control activities pursuant to the control plan focused on the following areas:

Public administration information systems

One of the priorities of the Office's control activity within the 2008 control plan lay in monitoring of the conditions that must be respected by every controller or other operator of a public administration information system. Control in this area concentrated on a diagnostic institution, a children's home with a school, a children's home, an educational care centre, an elementary school and a school canteen. The control has not yet been completed.

Information systems in the area of justice and state attorney's offices

Based on the experience obtained by the Office from a control performed in this area during the previous year, it continued to perform its competence in this area in 2008.

Multinational information systems

A meeting of the joint supervisory bodies for the Schengen Information System and for the Customs Information System, as well as a meeting of the EURODAC Coordination Group, indicated that these bodies would again initiate coordinated inspections of the mentioned systems in 2008. Also given the accession of the Czech Republic to the Schengen Area, the Office considered it necessary to perform these controls.

Personal data processing in the use of camera surveillance systems

The Office concentrates particularly on the area of health care and provision of social services. The controls have not yet been fully completed, but partial findings can nonetheless be presented.

Consumer protection

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

Control activities based on instructions of the President of the Office

In addition to the fundamental directions of controls undertaken by the Office, which are defined in the control plan for each year, the Office also pursues certain socially important control activities based on instructions of the President of the Office to the individual inspectors, who then follow these instructions in the performance of their control competence. Based on the President's instruction, in the period from February 6, 2008 to April 22, 2008, an inspector of the Office carried out a control of Evropský investiční holding, a.s, which operates, inter alia, the Savoy Hotel in Prague. According to publicly available information, a recording made by the camera surveillance system operated in the hotel had been publicly disclosed. Therefore, the President of the Office issued an instruction to perform control of personal data processing in this camera surveillance system. Violations of the Personal Data Protection Act and the Labour Code were found during the control.

Findings from controls

PUBLIC ADMINISTRATION INFORMATION SYSTEMS

Personal data and public administration

Instigations that were found justified and that triggered an action by the Office were concerned with publication of personal data obtained by a public administrative authority within the performance of public administration, operation of paid parking zones and the use of the information system of the register of population. Administrative proceedings were pursued both on the basis of controls and directly on the basis of selected instigations. Pursuant to the Act No. 133/2000 Coll., on register of population and birth numbers and on amendments of certain acts, as amended (hereinafter the "Register of Population Act"), a birth number may be used only for activities of the Ministries, other administrative authorities, bodies entrusted with the performance of state administration and courts, for activities that follow from their statutory duties and for activities of the notaries for the needs of keeping the Central Records of Wills. However, it must be noted at the same time that, although administrative authorities are authorized to use birth numbers, this provision cannot be construed in that they may use a birth number without any limitation. In its use, they must respect the Personal Data Protection Act, according to which a controller is obliged to process personal data only in accordance with the purpose for which they were collected.

Pursuant to the Code of Administrative Procedure, the reasoning of a decision includes the reasons for the operative part or operative parts of a decision; the basis for issuing a decision; considerations employed by the administrative body in their evaluation and in interpretation of the legal regulations; and information on the manner in which the administrative body dealt with the proposals and objections of the parties and their statements related to the basis for the decision. It follows from the above that the reasoning of a decision should not include unambiguous identification of the party to the proceedings, which is required in the operative part of the decision. In the operative part, a complainant was identified only through her name, surname, date of birth and address of residence, i.e. in accordance with the Code of Administrative Procedure.

Controls concerned with the register of population correspond to the position of this official source of personal data of all the inhabitants of the Czech Republic and the fact that this source is being used by a number of bodies of public administration, both on the basis of the Act on Register of Population and on the basis of several dozen special laws.

Four complaints were delivered to the Office in respect of **launching of paid parking zones in the Capital of Prague**. Five controls were closed in early 2008. Four administrative proceedings were held on the basis of the control findings.

In one of these proceedings, it was noted that, when issuing parking cards for paid parking zones, the relevant municipal authority failed to inform the party to the proceedings of its rights related to the relevant data processing, particularly of the manner of processing personal data and parties to which the personal data may be disclosed. Furthermore, it failed to inform the party of the right to access the personal data and of the right to have the personal data corrected, and also failed to submit a document attesting to the fact that it had adopted technical and organizational measures to secure personal data protection of the applicants, whereby it breached the duty to inform data subjects of the scope and purpose of personal data processing, and by whom and in what manner the data would be processed and to whom the data could be disclosed. It also failed to comply with the duty to inform the party of the right to access the personal data, the right to have the personal data corrected, as well as other rights stipulated in Article 21 of the aforementioned Act, and to advise it as to whether the provision of personal data was obligatory or voluntary. Moreover, it breached the duty to process and document the technical and organizational measures adopted and implemented to secure personal data protection of the data subjects in accordance with the Act and other legal regulations. A fine in the amount of CZK 12,000 was imposed on the authority for breach of these duties. It was ascertained within the performed control that the documented security measure had been implemented and was continuously and permanently employed.

A further three proceedings were pursued within the same scope. One of these proceedings was pursued because the party to the proceedings had copied, as a personal data controller, in proceedings on issuing parking cards for paid parking zones, the identity cards of the applicants and identity cards of the persons acting on their behalf, while not having proven the consent of any data subject to the acquisition of a copy of the identity card for the processing of his/her personal data. One of these proceedings was also pursued, because a party to the proceedings failed to stipulate the means and manner of processing of personal data of the population – the applicants for parking cards. Neither the regulation nor the Methodology of Issuing Parking Cards for the paid parking zones issued by this party includes any provisions that could be considered to determine the manner or means of personal data processing. A binding guideline for issuing parking cards for paid parking zones issued by a party to the proceedings determines the manner and means of processing for selected documents which are required from the applicant in case that the applicant does not submit the original or certified copy of an extract from the Commercial Register and Land Registry. The basic form of determination of the means and manner of personal data processing thus consists in a decision of the party to the proceedings to acquire and use a system processing personal data of the holders of parking cards. This is followed by partial decisions that need to be inferred from the ascertained functionality of the employed means of automated processing and from the procedures that are described, to any degree, in the documents ascertained by municipal authorities. In the documentary part, only those means and manners that are recorded, in some form, in the minutes of the meetings between the party to the proceedings and the mayors of the city wards can be considered to be determined. The mentioned procedure cannot be deemed to be

due determination of the means and manners of personal data processing within the meaning of Article 5 (1) (b) of the Personal Data Protection Act.

Furthermore, the party failed to incorporate the requirements on security measures in the agreements with the supplier of the application software, where personal data of the applicants for a parking card were being processed, and it neither drew up nor secured documentation in the sense of Article 13 (3) and (4) of the Personal Data Protection Act and did not deal with the relationship to the measures adopted by the city wards. It provided no document to demonstrate that it had adopted a measure to secure personal data of data subjects within the meaning of Article 13 (1) and (2) of the Act so as to avoid any unauthorized or accidental access to their personal data, or their change, destruction or loss, unauthorized transfers, other unauthorized processing, as well as other misuse of these personal data. Within automated processing, the party failed to ensure, in the sense of Article 13 (4) of the Personal Data Protection Act, the acquisition of electronic records that would allow for identifying and verifying as to when, by whom and for what reason the personal data were recorded or otherwise processed. A fine of CZK 70,000 was imposed in these proceedings; fines of CZK 20,000 and 10,000, respectively, were imposed in the other proceedings.

Processing of personal data in public administration was a frequent subject of inquiries and requests for consultations. Inquiries were mostly made by employees of the individual public administration authorities; however, a number of inquiries were also submitted by members of municipal assemblies. Several public administrative authorities addressed the Office with a request for an opinion on processing of personal data that were simultaneously governed by several legal regulations. They were interested, e.g., in the use of the information system of the register of population for initiating administrative proceedings. In this relation, the Office expressed the opinion that the data required for due identification of a natural or legal person for the purposes of initiating administrative proceedings must be obtained particularly within the performance of control competencies; the absence of such a finding, in itself, cannot be a ground for seeking data in information system kept by other authorities.

Certain issues in personal data processing by municipal and city authorities in the records kept by them are related to the relationships between the professional personnel and the members of the assemblies. While the former are usually aware of the legal regulations and obey them, the members of assemblies often have different requirements and believe that, on the basis of their position, they ought to know almost everything that is going on in "their" organization. The mentioned issue was repeatedly dealt with in relation to a long-term employee of one of the municipal authorities in the South-Bohemian Region in 2008.

The principle that the **public administration may do only what the law requires or allows cannot be avoided even with the potential consent of the data subject**, which was an explanation put forth, undoubtedly in good faith, by a Prague hospital with the aim of remedying a legislative shortcoming in the provision of birth numbers of newborn babies in the chain Ministry of Interior – Registry of Births – maternity hospital – health insurance company. The proposed model, where the **Registry of Births would obtain the consent of the statutory representatives of the newborn babies to the disclosure of their birth number to the maternity hospital, thus could not be recommended by the Office. Remedy must be ensured by the Ministry of the Interior,** which was informed of the issue in February 2008.

A relatively urgent need for clarification has been shown, in the long term, in the **provision of personal data pursuant to Act No. 106/1999 Coll., on free access to information**. The Office has repeatedly explained Article 8a of the cited Act, which refers to the procedure pursuant to the Personal Data Protection Act. The obliged entities also make mistakes in that they publish personal data of the applicant simultaneously with publishing their answer, which is not admissible without consent of the data subject. There are also **tendencies, based on various motivations, to intentionally not provide the required information, while making a clearly inappropriate reference to duties pursuant to the Personal Data Protection Act, such as in the case of a request for disclosure of the price of a municipal apartment that was being sold into personal ownership, where the price had been determined by a court expert**. Personal data of the current tenant are irrelevant in this respect and may not be disclosed in this relation without his consent; however, a person potentially interested in the purchase of the apartment is undoubtedly legally entitled to the disclosure of the expert estimate. Inquires were also repeatedly made as to the conditions of **disclosure of personal data from various records to the municipal or city police force**. In one case, the city police required personal data of a dog owner in order to perform control of compliance with the edicts on local dog fees, or to perform further inquiries concerning an attack by a dog belonging to an unknown owner. On these grounds, the police considered it suitable to have access to the records of the municipal authority also outside the official hours. The Office adopted a legal opinion that this could be possible in public interest; nevertheless, the records may not include data exceeding the scope stipulated by the legal regulations, which is formalized in the reporting card. Otherwise, this would breach the duty to collect personal data only within the scope required to fulfil the specified purpose, i.e. collection of local fees. At the same time, the municipal police may obtain data only within the scope that is essential for their further investigation. Remote access to the municipal records by the municipal police was permitted only by an amendment to the Municipal Police Act, which has been valid since January 1, 2009. However, it is necessary to resolve technical aspects to ensure that the municipal police have access only to the basic identification data of the dog owners, i.e. the name, surname, date of birth, place of residence and the fact as to whether or not the fee has been paid. This legal opinion was also presented at a meeting called by the Ministry of Finance. In the presence of representatives of the Ministry of the Interior, it was stated on November 26, 2008 that the two ministries would prepare an expert opinion that would be sent to the Office for comments and, subsequently, distributed via various information channels to the municipal authorities, with the aim to unify this access on the basis of absolutely transparent legal grounds.

Inquiries are also concerned with **issues following from newly effective laws. An application for a standpoint on the cooperation of the Archives of the Ministry of Foreign Affairs of the Czech Republic (AMFA) with the Institute for the Study of Totalitarian Regimes (ISTR)** pursuant to Article 5 (2) of Act No. 181/2007 Coll. on the Institute for the Study of Totalitarian Regimes and on the Archives of Security Corps and amending certain laws, which came into effect on August 1, 2007, can serve as an example in this respect. The Office noted, inter alia, that the mentioned Act does not relieve the entities that have the duty to cooperate pursuant to Article 5 (2) of the Act from the duty to comply with the requirements of the Personal Data Protection Act and Act No. 499/2004 Coll., on archives and the filing service. The mentioned legal regulations do not stipulate any different regime of processing of personal data in the activities of the ISTR. The disclosure of materials from the archives is generally permitted by Article 5 (2) (a) of the Personal Data Protection Act, which authorizes the personal data controllers

to process data also without the consent of the data subject where this is necessary for fulfilment of the controller's legal duty. Furthermore, the Office pointed out special protection of sensitive data within the meaning of Article 4 (b) of the Personal Data Protection Act, which is provided in relation to living natural persons, not only in this Act, but also in Article 37 (2) of the Archives and Filing Service Act; it stated that, where sensitive data of living persons are part of the archive materials, the AMFA is not obliged to provide these data to the ISTR without the consent of the affected persons. The Office reiterated that the aforementioned fact means that only certain information, rather than the entire documents, may be refused. As regards the character of information on membership of the Communist Party with respect to the purpose of establishment of the ISTR and the subject of its research, the Office noted that it could be concluded that membership of the Communist Party prior to 1990 need not be considered sensitive data within the meaning of the mentioned regulation.

Tax authorities, tax directorates and Ministry of Finance

The performed controls indicated several serious issues: Firstly, it has been shown that the tax administration is so closely interconnected that individual sectors cannot be controlled separately. Control was carried out at two tax authorities and the competent tax directorates; a further control is now pending at the Ministry of Finance. Furthermore, one incidental control of tax authorities has been completed, while another has been suspended due to the problems described below. The first issue encountered in the control lay in interpretation of Article 3 (6) (f) of the Personal Data Protection Act. The provisions of Article 5 (1) and Articles 11 and 12 do not apply to processing of personal data that are required for the fulfilment of the duties of controllers stipulated by special laws to secure an important financial interest of the Czech Republic or of the European Union, including particularly the stability of the financial market and currency, the functioning of circulation of money and payment relations, as well as budgetary and fiscal measures, where various examples are set out in the footnote, including Act No. 218/2000 Coll., on budgetary rules and on amendment to some related laws (budgetary rules), as amended, Act No. 250/2000 Coll., on budgetary rules of local budgets, as amended, Act No. 6/1993 Coll., on the Czech National Bank, as amended, and Act No. 212/1992 Coll., on the tax system, as amended by Act No. 302/1993 Coll., but not Act No. 337/1992 Coll., on administration of taxes and fees (hereinafter the "Tax Administration Act").

In the opinion of the Office, which follows from the aforementioned provision of the Personal Data Protection Act, general tax administration does not fall within the scope of the statutory exemption, as it does not involve an important financial interest of the Czech Republic or of the European Union. When assessing personal data protection in the tax sphere, it must be noted that application of the Tax Administration Act limits the right to protection of privacy of individuals (Art. 7 of the Charter) and that application of the provisions on limits of fundamental rights and freedoms must not interfere with their substance and sense. This means that a tax administrator must take measures required for correct and full determination, assessment and fulfilment of tax liabilities, while putting emphasis on not interfering with the substance and sense of the right to protection of privacy of individuals (Art. 4 of the Charter). The extensive powers in ascertaining facts that are decisive for due tax assessment and the right to protection of privacy further support the legitimacy of the Office's competence related to the supervisory activities in administration of taxes and fees.

Another issue is related to the non-disclosure duty vis-ą-vis inspectors. The inspectors relied on Article 2 (5) of the Tax Administration Act: Any person involved in tax proceedings in any way whatsoever is obliged to maintain confidentiality of all facts learnt in or in relation to the proceedings; however, this duty does not relieve the tax administrator of the duty to provide data to **a person who proves that (s)he is entitled to obtain these data pursuant to a special regulation** (including, indeed, the Personal Data Protection Act).

In order for the Office's inspectors to be able to verify as to whether or not the complainant's personal data are being processed in conformity with the law, they must be able to ascertain whether the company's tax file actually contains personal data of the complainant that are in no way related to the company's tax liability. The competent tax authority is trying to avoid this. On the contrary, the inspectors are attempting to enforce their powers by imposing procedural fines.

Another fundamental variance is related to Article 12 of the Personal Data Protection Act, according to which each data subject has the right to know what personal data are being processed in respect of him or her; furthermore, if (s)he believes that this processing is at variance with protection of private and personal lives of data subjects or at variance with the Personal Data Protection Act, particularly if the personal data are inaccurate with respect to the purpose of their processing, (s)he may request an explanation and, as appropriate, request that such processing be discontinued (Article 21 of the Personal Data Protection Act). The sense of the mentioned provisions lies in protection against unlawful collection, disclosure or other misuse of personal data (Art. 10 of the Charter). The personal data within the scope in which they have been collected and are being processed on a taxpayer must be essential for tax administration.

Tax authorities object by referring to Article 23 of the Tax Administration Act, or rather its incorrect construction, where they argue that the data subject is not entitled to inspect its non-public part. In this respect, it should be noted that it is often up to the specific tax authority and its rules, or even a specific employee of the tax administration, as to what documents it will include in the public part, on the one hand, and in the non-public part, on the other hand.

According to the interpretation contained in judgment 1Afs 94/2006 – 60 of the Supreme Administrative Court, the limit for inspection of the non-public part is based on protection of information concerning other entities: The objective of the mentioned limitations clearly lies in protection of information concerning other entities which the tax administrator has available and which it may use, given its suitability, in assessing a tax with the use of relevant tools. However, if the tax administrator bases the assessment of a tax liability only on data concerning the applicant himself, there is no reason to refuse information to the applicant as regards the tool that was used by the tax administrator to determine the amount of the tax. In the control, the Office also pointed out the greater scope of protection in the processing of sensitive data, such as conviction of a crime or the state of health.

The entire tax administration is now working on a uniform Automated Tax Information System of territorial tax authorities in the Czech Republic (ATIS). Especially in control of potential misuse of personal data of the tax administration, the inspectors of the Office focused on compliance with a new provision of the Personal Data Protection Act, namely Article 13 (4) (c) of the Act: In the area of automated personal data processing, the controllers are obliged to acquire electronic records that allow for identifying and verifying as to when, by whom and for what reason the personal data were recorded or otherwise processed. The control at the Ministry of Finance was later initiated on these grounds. Two complaints were lodged with the Office during the mentioned controls: one of

them was concerned with suspected misuse of personal data obtained from the tax administration for private purposes, while the other was related to processing, in the tax file, of personal data which were not connected in any way with tax administration.

Case studies – further cases

Research on persons staying in facilities for institutional and protective care until their adult age

The Government of the Czech Republic required, in its resolution, that the National Committee for Prevention of Crime carry out research on further destiny of all the persons who had stayed, until their adult age, in educational facilities for the performance of institutional care or protective care and left them between 1995 and 2004 to join normal society. The research was focused particularly on the degree of their conflicts with the laws and the potential connection with the institutional care provided to these persons and their difficult transition to normal life, or their criminal careers.

The data were collected from March 2005 and they included, in addition to birth number, twelve pieces of information, which were collected through a questionnaire drawn up by the relevant department and sent by electronic mail on each of 17,454 affected persons: sex; age when placed in institutional care; type of measure ordered; type of institution in which the relevant person was placed; length of stay in the facility including contractual stay; age when leaving the institution; reason for departure; environment to which the person left; number of short-term escapes; number of long-term escapes; number of days during a short-term escape; number of days during a long-term escape; and also the numerical designation of the diagnostic office by whose employee the collected data were gathered. The collected birth numbers served for identification of the affected persons. Electronic mail was not used in the transfer of the collected data from the individual facilities to the diagnostic institutes. The diagnostic institutions checked the data collected within their jurisdiction.

The data were then combined for the entire territory of the Czech Republic. The objective of the combination was to create a set of data for further analysis within the research. It was possible to separate the set of birth numbers from this set for the purpose of submitting it to the competent authority for the purpose of supplementing data on criminal activities pursued by the given persons.

The control ascertained that consent to personal data processing was not obtained in the research from the persons whose personal data were being processed. The Act on the Implementation of Institutional Training or Protective Training in Educational Facilities and on Preventative Training Care in Educational Facilities stipulates that the facilities may provide information on the children only to the diagnostic institution in whose jurisdiction they are located, to statutory representatives and to authorities of social and legal care for children.

The public administration authority processed personal data for a purpose other than for which they had been collected, without prior consent of the data subjects. The controlled entity did not respect the duty following from the Personal Data Protection Act not to combine personal data that were obtained for various purposes. **The public administration authority, as the controller, proceeded at variance with the Personal Data Protection Act in the processing of personal data of the affected persons (minors)**, because it failed to maintain personal data only for a period required for the purpose of their processing, failed to

process personal data only in accordance with the purpose for which they were collected, without prior consent of the data subjects, combined personal data that were obtained for various purposes, failed to process sensitive data only within the limits of authorization stipulated in the Personal Data Protection Act and failed to destroy personal data once the purpose for which they were processed ceased to exist.

The control proved that the mentioned conduct of the public administrative authority violated certain provisions of the Personal Data Protection **Act and, therefore, a remedial measure was imposed**.

HEALTH CARE

A special legal regulation (Act No. 20/1966 Coll., on public health care) stipulates very precise (and also strict) conditions for handling medical documentation. Very specific conditions are also set out in this relation for processing sensitive personal data on the state of health. Nevertheless, it is relatively common for healthcare facilities (including, in the sense of the Act on Public Health Care, private physicians) to disrespect the statutory rules and thus breach the duties stipulated by the Personal Data Protection Act. In its supervisory activities, the Office also relies on a number of European instruments, such as:

- Proposal for a Directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare (COM(2008) 414 final, issued by the Commission on July 2, 2008);

- Working Document on the processing of personal data relating to health in electronic health records (EHR) (document WP 131 issued by the Article 29 Working Party for Data Protection (WP 29) on February 15, 2007);

- European Standards on Confidentiality and Privacy in Healthcare (issued by EuroSOCAP in May 2006);

- Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: e-Health - Making Healthcare Better For European Citizens: An Action Plan For a European E-Health Area (COM(2004)0356 final issued by the Commission on April 30, 2004).

In 2008, the Office provided a consultation for the area of health care, where it adopted a negative standpoint on the duty, imposed on private physicians by the Ministry of Health, to state, within the stamp used by them, also personal data unrelated to the provision of health care, such as the place of residence and private telephone number. Following a notice by the Office, the Ministry provided for a remedy.

The Office also adopted a negative legal opinion on the publishing of personal data of medical commissions' members, where it opposed to the opinion of the Ministry of Health that this could be done only with the doctors' consent. The conclusion reached by the Office, i.e. that the patient should be aware, as for court experts, of who made a decision related to him or her, was also supported by employees of the Ombudsman's Office at a joint meeting in July 2008. In respect of transfers of birth numbers of newborn children in the chain Ministry of Interior – Registry of Births - maternity hospital – health insurance company, it was stated that the current state of affairs was not resolved in the legislation and that the maternity hospital indeed had to await information from the newborn's statutory representative. In relation to the aforementioned issue, the Office concluded that the current legislation did not stipulate (apart from consent of the statutory re-

presentative of the newborn child to the disclosure of the child's birth number) any legal grounds for the provision of birth numbers of newborn children by the health insurance company to the relevant healthcare facility. This fact, i.e. the existence of a legislative gap in the provisions regulating the relationships of the parties involved in the assignment of a birth number and its subsequent use in the provision of health care, has long been pointed out by the Office; nevertheless, its motions and comments aimed to resolving the issue have not been successful to date.

Although a majority of instances of data processing in the area of health care are regulated by a special law (Act on Public Health Care) and are not subject to the notification duty pursuant to the Personal Data Protection Act, the Office was also notified of processing subject to the notification duty. For example, 4 notifications concerning medical research were registered in 2008. The first notification included an application for registration of a camera surveillance system in the room of patients suffering from epileptic seizures. As it is not possible to stay with the patient in his room 24 hours a day, the camera surveillance system helps the medical personnel to care for the patient. A nurse can identify an epileptic seizure in time and provide aid to the patient. At the same time, the cause of the seizure can be determined from the recording (helping medical research in this area).

The second registration is related to adult genetics, where a client contacts the given company, undergoes swab of the mucous membrane on the inner part of the gums, with subsequent full genetic analysis. It can be ascertained in this way whether or not the client has any congenital dispositions for approx. 20 diseases (what is the risk that the client could contract the disease). Suitable prevention is then recommended on the basis of the results.

The third and fourth notices are related to scientific research in the fields of medicine and genealogy with the aim of determining the frequency of a certain trait in the population. On the basis of his inclusion in the Czech DNA database, the client can ascertain the origin of his ancestors, find lost relatives, determine the likelihood of a family relationship with another person, identify predispositions of human traits and determine the biological relationships with other persons.

The Office received numerous complaints in the area of health care; a prevailing shortcoming was related to the disclosure of personal data of newborn children, and their statutory representatives, to insurance brokers, who then unethically offered products of financial institutions. However, as the sources of this information had not been proven, the Office could not apply its supervisory competence.

The last wave of complaints was recorded in November 2008 in relation to the website www.znamylekar.cz, which drew the attention of commercial TV Nova. The author of the website used data from the public Commercial Register to compile a database of thousands of private physicians, where the readers evaluated their doctors. Some comments are on the boundary of crime (e.g. defamation) and are apparently at variance with the Civil Code; however, they cannot be classified as violation of the Personal Data Protection Act, as the readers are not in the position of controller or processor of personal data. To date, only in one instance did the author of the website collect personal data not included in the Commercial Register or any other public register (a private mobile telephone number of a doctor) without the consent of the data subject.

A number of violations of the Personal Data Protection Act were found within the controls performed in 2008:

With respect to hospital information systems (HIS), it was stated that a hospital was obliged to process data in medical documentations pursuant to Article 67a of the Act on Public Health Care and, therefore, it was subject to an exempti-

on pursuant to Article 9 (c) of the Personal Data Protection Act applicable to processing of sensitive data, which include data on the state of health. Nevertheless, a hospital, as a personal data controller, has the duties following from the Personal Data Protection Act, particularly in preventing unauthorized or accidental access to personal data. Information included in the HIS serves physicians as a basis for their further work with the patient. The medical documentation of a specific patient can be perused only by the doctor who actually treats the patient.

The aspect of securing the HIS can be summarized in three preconditions:

– No information on a patient of a given name or any further information on his state of health can be found without knowledge of the insurance (birth) number.
– Individual healthcare professionals have various levels of authorization to peruse medical documentation.
– It can be ascertained as to who has accessed the medical documentation of a given patient, who has read it, changed it, supplemented it or made an extract from it, or cancelled anything in the documentation.

Judicial review

Court proceedings against a polyclinic were closed. These proceedings related to an action lodged in 2007 against a decision of the Office, which imposed, on the polyclinic, a fine of CZK 1,750,000 for breach of the duty pursuant to Article 13 (1) of the Personal Data Protection Act, in relation to finding a medical documentation (medical cards) of approx. 2,000 patients, which occurred at the end of 2005 at a waste collection yard. This documentation was identified as originating from the building of a health-care facility – polyclinic. The Municipal Court in Prague discontinued the proceedings on the action lodged by the polyclinic by resolution on the grounds of failure to pay the court fee and the Supreme Administrative Court subsequently (March 2008) dismissed a cassation appeal lodged by the polyclinic against this resolution.

INFORMATION SYSTEMS IN THE AREA OF JUSTICE AND STATE ATTORNEY'S OFFICES

Personal data and activities of distrainers

In 2008, the Office encountered personal data processing in relation to activities of distrainers both within consultations and also in the area of control proceedings, administrative punishment and (subsequently) also in the framework of judicial review of decisions of the Office. Particularly the manner of identification of the obliged persons within distraint proceedings and publication or making accessible of personal data of the obliged persons by distrainers appear to be problematic in this respect. In the area of administrative punishment, the activities of distrainers in personal data processing cannot be considered a marginal issue. In addition to the mentioned disclosure of personal data of the obliged persons in distraint proceeding to unauthorized persons, this relates particularly to specific procedures of distrainers or their employees in the performance of duties stipulated by the law.

Disclosure of personal data of parties to distraint proceedings by distrainers

It was determined by means of a control as to whether and how distrainers, who are personal data controllers, perform duties stipulated by the law – i.e. whether they process data only in accordance with the purpose for which they were collected.

A shortcoming was also found in the work of a distrainer who had submitted copies of documents from the file containing personal data of the obliged persons and thus disclosed the data to an unauthorized person. It was also ascertained that the distrainer had failed to obtain consent of the obliged person to this step, as would be required by the Personal Data Protection Act. The control proved that the mentioned conduct of the court distrainer violated the law.

A fine was imposed on the distrainer in administrative proceedings for the mentioned administrative offense.

Information duty of distrainers vis-à-vis the obliged party in personal data protection

It was determined through the control that, when the obliged person inspected the file, the court distrainer acquired and included, in the mentioned file, a copy of one side of the obliged person's identity card, containing, inter alia, the latter's photograph, for the purposes of current and future identification of the obliged person. At the same time, the distrainer notified the obliged person that he did so for the purpose of his identification and that the acquired copy would be included in the file related to the distraint proceedings against his assets. The distrainer provided no further information to the obliged person in this respect. While the distrainer had obtained an implicit consent of the obliged person, he had not provided the latter, as a data subject, with information within the scope required by the Personal Data Protection Act in case of their collection of personal data. The control proved that the mentioned conduct of the court distrainer had violated the Personal Data Protection Act. A fine was imposed in administrative proceedings

Unauthorized disclosure of personal data of the obliged persons from the distraint file to other persons

On the basis of instigation, the office dealt with a case where, when inspecting the file, the complainant became acquainted with the contents of a document that contained personal data of other persons (identification details, including birth numbers) and further information.

Personal data of other persons were also disclosed to the obliged person during consultation of the file. However, only personal data related to the distraint proceedings should have remained accessible when being included in the file. The court distrainer thus breached his non-disclosure duty and also disclosed personal data with which he had become acquainted in the distraint activities to unauthorized persons. Thus, as a personal data controller, the court distrainer had failed to adopt measures preventing unauthorized access to personal data. A fine was imposed in administrative proceedings.

Disclosure of personal data of the obliged persons from the register of population

A court distrainer who was entrusted with performance of the distraint proceedings provided the entitled party with a copy of an extract from the central register of population related to the obliged person. The Register of Population Act stipulates that entities that obtain personal data from an information system (the information system of the register of population) pursuant to the special legal regulation (in the given case, the Act on Court Distrainers and Distraint – the Distraint Rules) are not authorized to collect, transfer and use these data outside the competence stipulated in the given regulation. Personal data protection in the distrainer's activities is secured, in the Distraint Rules, also through the duty of the distrainer to maintain confidentiality of all facts learnt by the distrainer in the performance of the distraint or other activity. Substantive provisions on handling of personal da-

ta related to the given case are also stipulated in the Distraint Rules, which set out, in an exhaustive manner, that a natural person must be identified in the application for distraint through his or her personal data within the scope of the name, surname and place of residence.

It was also determined through the control that the website of the Distrainer's office included an instruction for identification of the obliged persons in applications for distraint by means of their birth numbers. These facts demonstrate that the court distrainer had failed to adopt measures to prevent, on the one hand, unauthorized transfer of personal data and, on the other hand, other unauthorized processing thereof, i.e. that he had failed to respect the duties imposed on him as a personal data controller.

The control proved that the mentioned conduct of the court distrainer had violated the provisions of the Personal Data Protection Act. A fine was imposed on the court distrainer for the mentioned conduct.

PERSONAL DATA PROCESSING AND THE ASPECTS OF DNA

The Office encountered the issue of treatment of DNA and the related processing of personal and sensitive data in both the private and public spheres in 2008. A number of important documents were available as a basis in the area of DNA, such as:

– "Implementing rules of Prüm Initiative should ensure accuracy in DNA and fingerprint data exchanges" (issued by the European Data Protection Supervisor (EDPS) on December 19, 2007);

– "Working Document on Genetic Data" (document WP 91 issued by the Article 29 Working Party for Data Protection (WP 29) on March 17, 2004);

– "International Declaration on Human Genetic Data" (document No. SHS/EST/03/CIB–10/3 issued by UNESCO on October 16, 2003);

– "Report of the International Bioethics Committee (IBC) on the Possibility of Elaborating a Universal Instrument on Bioethics" (document No. SHS/EST/02/CIB–9/5 (Rev. 3) issued by UNESCO on June 13, 2003).

National DNA database

Control of the Criminological Institute of the Police of the Czech Republic, which processes personal and sensitive data in the **National DNA Database** (hereinafter NDD), was carried out on the basis of the Office's control plan in the 2006-2008 period.

A special law, i.e., at the time of the control, Act No. 283/1991 Coll., on the Police of the Czech Republic, authorized a police officer who, in performing the tasks of the police, could not obtain personal information permitting further identification in any other manner, with respect to persons accused of an offence and persons serving imprisonment for an intentional offence, to take biological samples permitting the obtaining of genetic information. Furthermore, the Police Act allowed for the combination of personal data and creation of databases; however, in personal data processing, the Police is authorized to process sensitive data where this is required, with respect to the nature of the crime, for the performance of the tasks of the Police in relation to criminal proceedings. Therefore, the Czech Police Act did not permit the creation of a database containing the profiles of all convicts.

Consequently, it was ruled that the creation of the National DNA Database violated Article 9 of the Personal Data Protection Act, as sensitive data had been col-

lected, further processed and maintained within a scope exceeding the statutory authorization. In these cases, it was necessary to request consent of the data subject as required by the Personal Data Protection Act.

While Act No. 273/2008 Coll., on the police, approved in 2008, no longer contains the aforementioned provisions in their original wording, it cannot be unambiguously stated that it allows for creating profiles of all persons convicted of an intentional crime, not to mention that the European institutions require that the Member States provide for processing of biometric data in a special law.

Recommendation No. R(92) 1 of the Committee of Ministers to Member States on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system stipulates: The establishment and operation of any DNA file for purposes of the investigation and prosecution of criminal offences should be regulated by law. A binding instruction of the Police President does not constitute such a legal regulation. This is an internal rule which does not adequately meet the precondition of subjecting the processing of sensitive data to a stricter regime, as mentioned in both the Personal Data Protection Act and the Police Act.

However, the rules following from the Police Act are quite unspecific and problematic and, therefore, with respect to all the ascertained facts, the establishment of the NDD requires separate legislation in the form of a law dealing with all the issues related to the establishment of the NDD. This law should, for example, stipulate an exhaustive list of persons from whom biological samples may be taken and stored in the NDD, provide for the procedure in destruction and removal of data from the NDD, stipulate exact rules on the retention period of the records in the NDD and also deal with the aspects of its control.

Furthermore, the aforementioned Recommendation supports the interpretation of the approach of inspectors to DNA sampling: The results of DNA analysis and the information so derived may however be retained where the individual concerned has been convicted of serious offences against the life, health and security of persons. Where the domestic law admits that samples may be taken without the consent of the suspect, such sampling should only be carried out if the circumstances of the case justify such action.

The Criminological Institute raised objections against the control protocol; however, the President of the Office, as the head of the control body, mostly dismissed these objections and confirmed the conclusions of the control, including the remedial measure consisting in destruction of the personal data processed at variance with the Personal Data Protection Act. The Office does not question the importance of the tasks of the Police, including prevention of crime. Nevertheless, in respect of the character of the data used by the Police in their activities and particularly with respect to the impact of processing of these data on the affected persons and in addition to the fact that these are sensitive data, account must also be taken of the entire context of processing – i.e. the potential relationship between the data subject and criminal conduct. The Office considers the requirement for the adoption of unambiguous norms to be essential. A secondary regulation must be considered only provisional.

Private company pursuing genetic testing

In 2007 and 2008, the Office also performed **control of a private company** that had **focused**, since its establishment, on **genetic testing** for the purposes of determining fatherhood, family relationships and analysis of deoxyribonucleic acid (hereinafter "DNA") for research and testing of genetically determined types of diseases and for predicting the effectiveness of their treatment.

After the submission of paternity tests and genographic tests to the clients, the company failed to destroy all the documents, which it may maintain, on the basis of the provisions of the Personal Data Protection Act, only for a term required to fulfil the purpose of their processing; the company also failed to destroy the related biological samples.

The company violated the provisions of the Personal Data Protection Act also in that it identified the patients, when maintaining personal data resulting from the clinical tests, through their names, surnames and birth numbers, although it stated in the informed consents to these tests that the information on the affected persons would be stored in the records, for the purposes of research, only under the initials of the name and the number assigned to the person at the beginning of the study. The aforementioned provision of the law requires that, in the use of personal data for scientific purposes, the right to protection against unauthorized infringement of the private and personal life of data subjects be secured and that the personal data be rendered anonymous, wherever possible. However, this was not so in the given case.

Prior to commencement of the control, the company failed to prove that the forms submitted to the clients would contain express consent of the client to personal data processing. It was ascertained that these documents had not contained even the information that had to be provided to the data subjects pursuant to the law.

Prior to the control, the company had performed paternity tests and tests of origin, without having notified this fact to the Office, and processed personal data as a personal data controller, without having notified the Office of this fact in writing prior to personal data processing.

The company, as a personal data controller, proceeded at variance with the Personal Data Protection Act in the processing of personal data of its clients, as it failed to maintain the personal data only for the term required for the purpose of their processing. Furthermore, in the use for scientific purposes, it failed to render the personal data anonymous wherever possible, it failed to process sensitive data only with the explicit consent of the data subject and having appropriately informed the data subject upon granting the consent. It also failed to inform and advise the data subject pursuant to Article 11 (1) and (2) and, as a personal data controller processing personal data, it had failed to notify the Office of this fact prior to commencement of personal data processing. The control proved that the mentioned conduct of the company had violated the Personal Data Protection Act. Objections were lodged against the control protocol with the President of the Office.

Second-instance proceedings

The President of the Office, as the head of the control body, mostly dismissed these objections against the control protocol and thus confirmed the conclusions resulting from the control, including the requirement for liquidation of the personal data processed at variance with the Personal Data Protection Act. Through the described conduct, the company committed administrative offenses consisting in breach of duties stipulated by the law, and was imposed a fine of CZK 90,000 for this violation. The order has already come into legal force.

MULTINATIONAL INFORMATION SYSTEMS

Personal data in common information systems of the EU

Membership of the Czech Republic in the European Union also results in obligations related to supervision of personal data processing in common information systems, which were established either on the basis of a special agreement to which the Czech Republic acceded or on the basis of secondary legislation stipulating the duty to contribute to such a system. At the supranational level, the appointed national supervisory authority then supervises the area of the country with respect to relevant processing pursuant to national legislation and also participates in central controls. Supervision of personal data processing in the central data files of the European Union is performed either by the joint supervisory body (JSB, JSA) or the co-operating national authorities and the European Personal Data Supervisor (EDPS). Activities at this level require that the Office be appropriately acquainted with processing carried out in the Czech Republic and on behalf of the Czech Republic. To this end, the control plan for 2008 includes control operations entitled Personal Data Processing in the Customs Information System, EURODAC Personal Data Processing and Personal Data Processing within the Schengen Information System. The Customs Information System and the Schengen Information System were established on the basis of an international treaty, while EURODAC is being operated on the basis of several Regulations.

Control focused on the national part of the Customs Information System, intended for the needs of prosecuting bodies, took place from April 15 to June 3, 2008 at the General Directorate of Customs. No breach of the duties stipulated by the Personal Data Protection Act, with application of the provisions of the Convention on Customs Information System, were found with respect to personal data processing. A procedure was found that did not correspond, in its consequences, to the requirements for personal data protection stipulated in the Convention on Customs Information System. The inspectors were not sure how the Customs Administration of the Czech Republic and the General Directorate of Customs could fulfil the purpose for which the system is operated when they did not use the system, although this was the basic intention of the relevant Convention. From the viewpoint of personal data protection, this procedure and approach endanger the quality of the processed personal data, also taking into account Article 13 (3) of the Convention on the Customs Information System, according to which the system is to be regarded in every Member State as a national data file being subject to the national provisions referred to in the Convention and the specific provisions of the Convention. Thus, the Customs Information System as such contains personal data that are subject to the requirement to ensure the level of protection pursuant to Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Failure to apply the procedures stipulated by the Convention on the Customs Information System does not correspond to the principles of data quality pursuant to Article 5 of Convention No. 108, particularly the principle pursuant to subparagraph a). It also does not correspond to the principle stipulated in Article 5 (d) of the same Convention, as it does not aim at keeping the processed personal data up to date, although this is undoubtedly required.

The control found some vaguely formulated information on the personal data retention period in the Customs Information System. However, the General Directorate of Customs, as the controlled entity, is not responsible for the wording of the provision of Article 12 of the Convention on the Customs Information System, which is the source of this information. The control was carried out with the use of findings obtained in the work of the Joint Supervisory Authority for Customs Information System (JSA Customs). Two controls were required to fulfil the aims of the con-

trol plan for 2008 with respect to EURODAC Personal Data Processing: control was commenced on August 19, 2008 at the Ministry of Interior with the aim to check personal data processing in the electronic database of fingerprints used within the Dublin System (EURODAC) and in processing of data on fingerprints of asylum seekers and applicants for granting international protection in general.

The evaluation of potential violation of the Personal Data Protection Act was based on Articles 5 (1) (d), 5 (3), 9, 11, 13 and 18 (2) of the Personal Data Protection Act. Furthermore, amongst other provisions, Article 5 (1) and (2) were also employed. The preconditions for application of other provisions of the Act were not fulfilled.

The controlled entity was found to have the duty pursuant to Article 18 (2) of the Personal Data Protection Act, i.e. the duty to ensure that the information on the purpose of processing, categories of personal data, categories of data subjects, categories of recipients and the data retention period, as explicitly stipulated categories of data, are disclosed directly to the data subject at the time of commencement of the actual processing of personal data. No publication of such data or their disclosure in some other form to persons other than the applicants for international protection was identified. This was found to be at variance with the Personal Data Protection Act. On the contrary, the formulation of the advice on the personal data retention period, intended for each individual data subject, giving rise to uncertainty as to the period for which personal data will be or may be kept, was not found by the inspector to be a shortcoming in the performance of duties pursuant to Article 18 (2) of the Personal Data Protection Act, resulting in breach of the duty, as the purpose pursued by the provisions of the Personal Data Protection Act has been attained – the recipient receives information on the data retention period.

Separate assessment of the national legislation and the ascertained state of affairs based on the applicable provisions of the three relevant Regulations (EC) have shown that the scope of data that are being collected in the Czech Republic according to the Asylum Act exceeds the scope stipulated by Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, which fact is not at variance with the Personal Data Protection Act.

Assessment was also made of the corresponding provisions of Convention No. 108 – given their direct applicability in a situation where the procedure of the controlled entity was challenged by a complaint of the data subject lodged pursuant to the Personal Data Protection Act.

The procedure of the Ministry, as described and documented in the control protocol, corresponds to the requirements set out in Article 5. No breach was found of any of the rights granted by Convention No. 108 to data subjects. The controlled processing is adequately secured from the viewpoint of data subjects, as guaranteed by the contracting parties of Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. The control was closed on October 24, 2008.

Based on the finding that the personal data processing that was the subject of this control also involved other entities, the inspector decided that control would also be performed at the Police of the Czech Republic.

The results of the both controls were directly used for the purposes of coordination meetings of the national authorities with the European Data Protection Supervisor. Control of personal data processing within the national part of the Schengen Information System was commenced on November 5, 2008, with envisaged

completion in early 2009 – so that the results of the control could be fully utilized in the performance of the tasks following for the Office from the Czech Presidency of the EU.

The outputs of the mentioned control will also be used within coordinated control agreed on the premises of the Joint Supervisory Authority for the Schengen Information System (JSA Schengen), which has gradually checked (at the central level and, through the national authorities, also at the national level), over the recent years, the individual areas of personal data processing in this information system and which currently focuses on checking the procedures pursuant to Art. 97 and 98 of the Convention implementing the Schengen Agreement.

An employee of the Office from the department responsible for international cooperation in the given area was also a member of the control team within all the control operations in this field. The control program allowed for obtaining basic documents for the provision of data required for monitoring and harmonization of personal data processing at the level of the EU.

In direct response to the requirements for cooperation in the performance of supervision over personal data processing pursuant to the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), control was carried out at the Police of the Czech Republic from May 12 to May 23, 2008 on the basis of the underlying documents provided by the Joint Supervisory Body of Europol.

It was found that the Police of the Czech Republic failed to proceed, in the processing of personal data stored in the Europol information system, in full conformity with the provisions of the Europol Convention. In one case, a shortcoming was found in assessment of permissibility of personal data processing on the basis of the Europol's competence related to a certain form of crime or its specific manifestations. All the preconditions for making an entry in the Europol information system, as stipulated by Article 2, were not met in respect of personal data processing and these preconditions were also not met later. No procedure contrary to Art. 21 (3) of the Europol Convention was found. Given the fact that the entry containing the personal data, with respect to which all the preconditions for entering them in the Europol information system kept pursuant to Art. 7 and 8 of the Europol Convention were not simultaneously met, was deleted and the personal data contained therein were destroyed during the control performed by the Office, no reasons for imposing a remedial measure were found.

PERSONAL DATA PROCESSING WITH THE USE OF SURVEILLANCE SYSTEMS

Camera surveillance systems and personal data processing

In 2008, the Office again paid great attention to the issue of personal data processing with the use of camera surveillance systems.

In general, it can be summarized that, most frequently, the use of camera surveillance systems is being justified by the protection of persons, protection of property, protection of public order, detection, prevention and prosecution of crime, obtaining evidence and fight against terrorism. Thus, these are legitimate reasons that promote, directly or indirectly, the protection of individuals; however, their privacy is being seriously endangered by the constantly increasing scope of monitoring.

The operators of camera surveillance systems are subject to the Personal Data Protection Act provided that they systematically process the obtained information within the meaning of Article 4 (e) of the Act. This is so in all cases where a

camera surveillance system (focused on monitoring of natural persons) is equipped with recording equipment, as, in that case, images of persons located at a certain time in the monitored area are systematically collected. It could also be assumed in the described context that these images are being further utilized; otherwise (should the images not be used), the recording equipment would lack any sense.

The right of the data subject to protection of his/her private and personal life may not be infringed in personal data processing that is necessary for the protection of the rights and legally protected interests of the controller. When evaluating this aspect of personal data processing, account must be taken of the location of cameras and their range, together with the character of the monitored areas and the operating circumstances, so that these do not result in processing that would inappropriately interfere with the private and personal lives of the data subjects.

At the same time, once the controller begins processing, he is fully responsible for ensuring that the personal data are processed in conformity with the duties imposed thereon by the Personal Data Protection Act; therefore, inter alia, the controller is obliged to process personal data only in accordance with the purpose for which the data were collected and in no case may he use them for any other purpose.

Registration notification of operation of camera surveillance systems

The number of registration notifications concerning the operation of camera surveillance systems again substantially increased in 2008. In relation to the process of registration of camera surveillance systems, the Office strives to take the path of awareness raising and prevention. Nevertheless, although to a lesser degree than in 2007, the registration notifications again encompassed processing contrary to the duties of the controllers stipulated by the Personal Data Protection Act (e.g. illegitimate purposes, inadequate performance of the duty to provide information, inappropriately long recordings retention period, clear infringement on the right to protection of privacy, etc.). The most serious shortcomings occurring in registration notifications include particularly incorrect assessment of the balance between the values that are to be protected by the camera surveillance system and the values that the camera surveillance system infringes. Inadequate utilization of other means that could attain the objective aimed at by the controller more effectively, as well as incorrect, in most cases excessively strict, interpretation of the term of privacy, resulting in insufficient account being taken of the relationship between the location of the camera and infringement on privacy, remain substantial issues.

Within evaluation of legality of use of a camera surveillance system, the Office employs the following decisive criteria:

• Whether the camera surveillance system does not inappropriately interfere with the right of the data subjects to protection of their personal lives.

• Whether the use of the camera surveillance system is indeed essential and whether it is actually the last resort and only legal option of attaining the set objective with respect to the circumstances of the case.

• Whether a recording from the camera surveillance system can attain the declared purpose.

The criteria are based on Decision of the Constitutional Court Pl. US 4/94 dealing with a mutual conflict of fundamental rights and freedoms (such as the right to privacy vs. the right to protection of property). It follows from the constitutional order and from the mentioned Decision that, although this is not envisaged by the Constitution as such, certain fundamental rights and freedoms could be limit-

ed in case of a mutual conflict. The following conditions can be used when assessing the possibility of limiting a fundamental right or freedom for the benefit of some other fundamental right or freedom, where the fulfilment of this condition gives priority to the relevant fundamental right or freedom: a) mutual comparison, b) examination of essence and significance (Art. 4 (4) of the Charter), and the following criteria can thus be determined:

• Criterion of suitability, i.e. whether the institute limiting a certain fundamental right allows for attaining the set objective (protection of some other fundamental right).

• Criterion of necessity, consisting in comparison of the legislative means limiting the right or freedom and other measures enabling the attainment of the same objective, while not infringing on fundamental rights and freedoms.

• Criterion of comparison of the importance of the two fundamental rights or freedoms that are in mutual conflict.

A number of registration decisions indicate that the operator and controller of a camera surveillance system makes a decision on its installation based on a "governance" approach, where he attributes rights only to himself, while disregarding the rights of others. The Office evaluates, in each individual case, as to whether temporary use of a camera surveillance system for detecting petty offenses and repeated vandalism is justified at a given place and time, or whether this is a futile and emergency measure.

Camera surveillance systems on public premises

Within registration notifications lodged in 2008, the Office was increasingly addressed by smaller municipalities that intended to operate a camera surveillance system on public premises (squares, streets, parks). The reason for such monitoring allegedly lay in ensuring public order and preventing and detecting crime. In these cases, the applicant is a municipality that has no municipal police force and is interested in operating a camera surveillance system on public premises, while pursuing an objective under public law. The Office issued a standpoint on this aspect in Journal No. 49/2008, where it concluded that personal data processing via camera surveillance systems with recording equipment operated by a municipality that has no municipal police force on public premises (squares, streets) for the purpose of prevention and prosecution of crime would be at variance with the applicable laws of the Czech Republic. The operation of a camera surveillance system on public premises for a public-law purpose is possible only through the Police of the Czech Republic or a municipal police force.

Instigations lodged by citizens were concerned with the operation of camera surveillance systems on publicly accessible premises, where criticism was aimed particularly at municipal and traffic safety camera surveillance systems that monitored the situation on squares, streets and roads.

Camera surveillance systems in apartment buildings

Based on an increasing number of accepted complaints, the Office issued standpoint No. 1/2008, "Installation of camera surveillance systems in residential buildings", which deals with the issue of operation of camera surveillance systems in residential buildings. The number of accepted registration notifications lodged by the owners of residential buildings substantially increased after publication of information on this subject. This was so regardless of whether the residential buildings were owned by municipalities, private entities, cooperatives,

etc. An increased number of instigations for control was an unwanted, but expected result of this measure. An increase in the number of complaints of this nature was noticed after publication of standpoint of the Office No. 1/2008, declaring the possibility of utilization of camera surveillance systems with recording equipment in residential buildings only with the consent of the tenants. A total of 13 of these complaints were referred for further analysis preceding control. Next year, the Office will gather public opinions related to the mentioned standpoint in the interests of ensuring a really effective application of the law.

Camera surveillance systems in hotels and restaurants

A workshop for invited managers of hotels throughout the Czech Republic took place on November 12, 2008 in cooperation with the Association of Hotels and Restaurants. It can be concluded that the presentations substantially contributed to understanding of the entire issue and, in the future, also to an increase in protection of the recorded personal data through camera surveillance systems with recording equipment. The Association of Hotels and Restaurants showed interest in continued cooperation with the Office.

Camera surveillance systems at workplaces

Frequent inquiries and complaints are related to the persisting problem of monitoring employees via cameras at the workplace, both in major institutions and factories and in minor private enterprises. These are often anonymous instigations; requests for non-disclosure of the complainant's name are also increasingly common. Complaints related to the operation of camera surveillance systems that are used to monitor solely employees, i.e. that indicate the possible violation of the Labour Code, are referred to the substantively competent authority, i.e. the State Labour Inspection Office.

Numerous complaints pointing out the operation of camera surveillance systems with recording equipment by natural persons who are not entrepreneurs, in a vast majority cases aimed at protection of own property of the given natural person, are being rejected as unjustified. It is explained to the complainants that the Personal Data Protection Act cannot apply, pursuant to its Article 3 (3), to personal data processing that is performed by a natural person exclusively for his or her personal needs. As certain cases indicated potential violation of Article 12 of Act No. 40/1964 Coll., the Civil Code, as amended, it was suggested that the complainants deal with this issue by lodging a civil-law action. Although the Office is obliged to deal with all petitions, general references made by anonymous complainants to the fact that a certain institution or a specific person operates a camera surveillance system, without specifying the substance of the suspected violation of the Personal Data Protection Act and whether the complainant has been harmed by the operation of the camera surveillance system, were rejected as unjustified.

Case studies

In 2008, the Office's inspectors carried out a number of investigations and over 40 controls which were concerned exclusively with the use of camera surveillance systems operated on various premises. These controls were carried out in governmental and municipal institutions, manufacturing premises, hospitals and residential buildings.

Evaluation was made within the controls, inter alia, of whether a school has the right to process personal data. It was stated that the use of a camera surveillance system with recording equipment is a considerably more serious intervention in the private and personal lives of the teachers and students of the school than detection of minor incidents. The school has undoubtedly a number of other options of preventing minor thefts and, particularly of resolving the issue of supervision in corridors, cloakrooms, etc., in order to avoid potential conflicts amongst the students. It was also not accepted that bullying amongst the students could be prevented through a camera surveillance system and continuous monitoring: The installed cameras would merely force bullying out to other places. This is true notwithstanding the fact that the school has not documented any case of bullying, also outside the range of cameras. Thus, this was rather a "retroactive" justification of installation of cameras, including misuse of the cliché of bullying. Based on the results of the control protocol and the imposed remedial measures, the school terminated the operation of the camera equipment during lessons and the equipment was used at a time when there was no school. Remedy was thus ensured and, instead of monitoring persons, the equipment is being used for surveillance of premises, and property and equipment of the school.

An anonymous complaint was also instigation for performing control at a detached workplace of a supervisory governmental agency. The declared purpose for the installation and operation of the camera surveillance system lay in protection of property, with emphasis on the protection of State property and particularly protection of health of employees, with justification that this was a supervisory governmental authority. Managers of the workplace failed to document any important case of theft or damage to the entrusted property or any physical attack against an employee of the authority. The acquired recordings contributed only to detection of theft of office equipment in a single case. Otherwise, the recordings had never been used, nor had they been submitted to the competent authorities. The authority acquired recordings without consent of the affected persons.

It was noted that recording of every-day conduct, not only of employees, but also of visitors, during the working hours, when the employees were present, for the purpose of protection of property, was clearly inappropriate infringement of privacy of the monitored persons. A remedial measure was imposed through the control protocol.

Another control was concerned with records on exceeding permitted velocity in city Z. The system of speed measurement over a certain distance, as operated in this city, constitutes infringement of the private and personal lives of the data subjects and is at variance with the requirements of Article 10 of the Act. Maintenance of information on all passing vehicles in the municipal information system has no basis in the law. Remedial measures were imposed, including, e.g., the requirement that the application "special-interest" vehicles be used only by the Police of the Czech Republic on the basis of duly pursued investigations, as neither the City of Zlín nor Zlín's municipal police had this authorization.

Pictorial documentation of operation of camera surveillance systems

All these cases involve the operation of a camera surveillance system with recording equipment where the recordings are being acquired without consent of the affected persons. The attached images were extracted from recordings that were seized within the control activities; image No. 6 was obtained from an internet daily newspaper. In order to render the persons anonymous, the faces on images Nos. 1, 2, 3, 5, 7 and 8 were subsequently defocused. The license plate of the vehicle on image No. 4 was also defocused.

Fig. 1
A camera on a staircase of an apartment building.
Purpose of monitoring – obtaining evidence for pursuing property disputes. (a recording was made of a culprit breaking a bush)

Fig. 2
A camera at the municipal authority, the department of traffic agendas.
Purpose of monitoring – protection of the city's property and ensuring safety of persons. (once we know what the client has in his wallet, we all feel safer…)

Fig. 3
A camera monitors the entrance to an apartment building through the parking garage.
Purpose of monitoring – protection of the parked vehicles against damage. (Where are the vehicles … ?)

Fig. 4
A camera in the underground parking garage of an apartment building.
Purpose of monitoring – protection of the parked vehicles against theft. (did you also recognize the driver-thief …?)

Fig. 5
Municipal lodging house for persons in need – corridor in front of the security guard's window.
Purpose of monitoring – protection of persons and property. (we must document what the visitors bring in …)

Fig. 6
Hotel Savoy – a camera in the hotel lobby.
Purpose of monitoring – safeguarding property and safety of accommodated persons. (we must have the right to document what famous people come to visit us…)

Fig. 7
Regional hospital, 31 cameras in the corridors.
Purpose of monitoring – prevention against entry by homeless people and against pickpockets.
(I am not homeless so I should feel safe under the camera …)

Fig. 8
Regional hospital, 31 cameras in the corridors.
Purpose of monitoring – prevention against entry by homeless people and against pickpockets.
(the hand on the girl's butt must be documented …!)

Fig. 9
Municipal hospital, camera in the office.
Purpose of monitoring – protection of property of the hospital.
(the resolution of the recording will surely contribute to detecting persons who copy documents without authorization…)

Fig. 10
Department store.
Purpose of monitoring – protection of property. (no comment …)

Administrative proceedings

In cases where the control indicated violation of the Personal Data Protection Act, proceedings were pursued, as required by the law, against the relevant parties for an administrative offence related to personal data processing with the use of a camera surveillance system.

A fine of CZK 200,000 was imposed on a State-owned company which processed personal data of its employees by means of an internal camera surveillance system in one of its production facilities for the purpose of identifying breach of the principles of manufacturing safety and control of performance of the output standards, confirmation of breakdowns and delays, all this without consent of the employees. In respect of data processing for these purposes and also for the purpose of identifying violations of the regulations on occupational safety and health protection and fire-prevention regulations and for the purpose of detection crime, the company failed to determine the period of retention of the acquired recordings, which it actually retained for a period of several months.

In relation to the operation of an internal and external camera surveillance system in the manufacturing facility, the company did not provide the data subjects with information on personal data processing. Furthermore, it maintained personal data set out in the "Evaluation of the video recording of March 5, 2005" in a plastic letter file in the foremen's room, where they were available to other employees also at times when the foremen were absent. For the purposes of keeping personnel records in the manufacturing facility, the company also processed superfluous personal data obtained from photographs of the employees, incorporated in the personal questionnaire and registry card. Finally, as the personal data controller, it failed to comply with its notification duty towards the Office in respect of the mentioned personal data processing in a camera surveillance system. The mentioned conduct breached the duties set out in Article 5 (2), Article 5 (1) (e), Article 11 (1), Article 13 (1), Article 5 (1) (d) and Article 16 of the Personal Data Protection Act. The party to the proceedings lodged an appeal against the decision on a fine; however, the President of the Office dismissed the appeal and the contested decision thus came into legal force. The Office's decision was subsequently challenged by an administrative action, which has not yet been ruled on by the competent court.

A fine of CZK 60,000 was imposed on a city that collected personal data of all persons present on the premises of the municipal authority without their consent and also at variance with the set purpose and beyond the scope required for fulfilment of the given purpose, i.e. protection of the city's property, prevention of corruption and protection of persons. Furthermore, it retained the personal data for a period of 5 days, which is not essential for the purpose of their processing, and also failed to comply with its duty to provide information. This decision of the first-instance administrative authority was again contested by an appeal, which was later dismissed by the President of the Office.

The number of proceedings pursuant to Article 17 of the Personal Data Protection Act and their results are indicated in a separate table describing the activities of the Office. Nevertheless, within this activity and in relation to the aspect of personal data processing through a recording from a camera surveillance system operated on public premises (such as squares and streets) of municipalities that do not have their own municipal police force, and for the purpose of preventing and detecting street crime and vandalism and with the aim of ensuring safety of citizens and visitors to the municipality, the Office came to the conclusion that any processing of personal data (video recordings) obtained through a camera surveillance system from publicly accessible places performed by an entity that is not authorized to this effect by the law (such authorized entities include the Police of the Czech Republic and, to a lesser degree, municipal police), for the purpose of preventing and detecting street crime, ensuring safety of citizens, etc., constitutes infringement of the private and personal lives of the data subjects, i.e. persons who are present in the monitored area and "live their everyday lives". From the viewpoint of constitutional law, this could constitute breach of the right to protection against unauthorized collection of personal data stipulated in Art. 10 (3) of the Charter of Fundamental Rights and Freedoms. Based on the above, it must be stated that the notified personal data processing also cannot be subject to the exemption set out in Article 5 (2) (e) of the Personal Data Protection Act.

Second-instance proceedings

The Office deals with assessment of camera surveillance systems within second-instance proceedings in three areas.

1. Objections raised against the control protocol in relation to controls of entities operating these systems.

2. Second-instance appellate proceedings against a decision of the Office on rejecting registration of personal data processing through a camera surveillance system (cf. Articles 16 and 17 of the Personal Data Protection Act).

3. Cases where a fine is imposed for personal data processing in this manner and this decision is again challenged by an appeal, which must be ruled on.

The second-instance proceedings pursued in 2008 included 5 cases of objections against the control protocol, 5 cases of appeal against a decision rejecting registration pursuant to Article 17 (2) of the Personal Data Protection Act and 5 cases of appeals against imposing a fine in relation to personal data processing through a camera surveillance system.

Within decision-making on objections, which falls within the statutory competence of the President of the Office, objections were assessed with respect to the conclusions of controls of camera surveillance system located in hotels, in a building of an authority and on the premises of a gallery, and also of a system utilized by a municipal police. In all cases, the main conclusions drawn by the inspectors of the Office were confirmed.

Judicial review

Two actions were lodged in 2008 against final decisions of the Office; through these actions, the affected entities claim a change within an extraordinary remedy. An action was lodged against a fine of CZK 200,000 imposed on a State-owned company which processed personal data of its employees by means of an internal camera surveillance system in one of its production facilities for the purpose of identifying breach of the principles of manufacturing safety and control of performance of the output standards, confirmation of breakdowns and delays, all this without consent of the employees. The action has not yet been discussed. Furthermore, an action was lodged with an administrative court against a decision on a fine (CZK 90,000) imposed on an elementary artistic school, which had installed a camera surveillance system and, with the use of the system, documented the behaviour of the employees, students and their company, employees of leased business premises and users of an apartment located in the school building, and also other persons visiting the school building. This action has also not been discussed yet.

At the end of the year, an action was also lodged with an administrative court against a decision of the President of the Office, whereby the President confirmed a fine in the amount of CZK 60,000 imposed on a city that monitored the premises of the city authority. This action will be discussed by the competent court in 2009 at the earliest.

CONSUMER PROTECTION

RFID technology – chip cards

In 2008, the Office controlled three entities utilizing the technology of RFID chips. All these entities were companies engaged in the provision of public passenger transport.

In these cases, the chip cards are used particularly as an electronic wallet and a certain form of a prepaid ticket. According to the operators of the cards, the reason for their introduction always lay in increasing the effectiveness and reduction of the operating costs. In none of the mentioned cases did the operator of the RFID technology declare the intention to "monitor" the card holders. It was shown that the operators were mostly unaware of the fact that this new technology encompassed, as a by-product, information on the place where the card holder was present at a given time. Thus, in the words of the Personal Data Protection Act, this constitutes collection of personal data of the holders of chip cards that does not correspond to the set purpose, without knowledge and thus also without consent of these persons. All the issuers of chip cards equipped with the RFID technology provide the same explanation for collecting these data. The reason lies solely in settlement of mutual financial transactions that take place through the card. The fact that personal data are simultaneously being processed is thus, from their viewpoint, necessary.

However, the Office is convinced that the basis for collection of these data rather consists in the initial approach of the issuers of the cards in their sale or distribution, when they record personal data of each holder of a chip card. In order to justify this procedure, they provide various explanations that are based mainly on reasons related to the statutory duty to provide transport services to the citizens. The Office has also encountered a statement that, for a transport company to be able to provide a discount, the citizen had to agree to submit, absolutely

"voluntarily", his personal data. It was ascertained within the performed controls that, while the legal regulations provide for the individual areas of provision of public transport, in no case do they stipulate the duty to keep records of the passengers. Of course, the Office checked all the reasons put forth with respect to personal data protection; however, it strived not to interfere with the control functions of the systems. It also noted the opinions of the complainants and certain opinions in the media that electronic control of passengers, connected with records of their personal data, are a consequence of a "governance" approach of the officers who make decisions as to by whom and for what amount the transport services may be used. In this respect they exert economic pressure: the annual difference in prices of transport, when used anonymously, on the one hand, and when allowing for monitoring, on the other hand, can reach several thousand crowns, which must be considered to force the citizens to obey. However, price issues fall outside the competence of the Office and fall within an area that may be controlled by the Czech Trade Inspection Authority and other competent governmental authorities.

However, from the viewpoint of the Personal Data Protection Act, it must be assessed whether the consent is not forced. According to the wording of the Personal Data Protection Act, the consent to personal data processing must be a free manifestation of the will of the data subject.

Control performed at the largest railway transport company was closed by imposing a remedial measure consisting in continuous anonymisation and destruction of all personal data collected on the passengers. Furthermore, a requirement was made for physical separation of the individual databases that are being kept in relation to the provision of transport services.

Controls performed at transport companies were concerned particularly with the authorization for and the legality of collecting personal data during the distribution or sale of the chip cards. It was ascertained that there was no statutory duty to collect and further process personal data in issuing chip cards. It has also been shown that transport documents – cards with an RFID chip – can be issued in a manner where the personal data including the name, surname and photograph are merely printed on the card and not stored in a database. A reason frequently put forth by the transport companies, i.e. that a list of persons to whom a card has been issued serves for these persons themselves in case of theft or loss of their card, so that the card can be readily and quickly blocked, thus preventing its misuse by an unauthorized person, must be rejected, as the law prefers means that do not interfere with privacy and do not threat personal data. Indeed, it is very easy to provide each card holder, upon issuing the card, with confirmation of delivery (payment) of the card, which may contain information on the type and number of the card, as well as the name and surname, if appropriate, which can be used to demonstrate the authorization to hold the card and the paid application. The card can be immediately blocked according to the number of the card set out on the document. However, in practice, the issuer of the card, as a personal data controller, himself makes a decision for the passenger, does not allow the passenger to manifest his free will and, moreover, patronises the citizen. It has been ascertained in controls that a chip card issued by a major transport company on the basis of a contract is being used by other transport companies that are involved in passenger transport within a certain region. The contracts are being used for mutual settlement on the basis of information that is obtained by "reading" the information through a card reader which is located in each contractual means of transport. Information is being obtained from the chip with respect to its number, place of boarding, place of disembarking, and date and hour of boarding, all this for the pur-

poses of mutual financial settlement. However, the chip number can be very easily used to identify the card holder, i.e. a specific natural person. Subsequently, it would not be difficult to find out where the given natural person – passenger – was located at a given time.

Based on the ascertained facts, the inspector of the Office ordered a remedial measure consisting in a change in the manner of keeping databases used to retain information on the movement of passengers. As of December 31, 2008, the Czech Railways announced that the remedial measure imposed had been complied with.

It can also be inferred from the course of the controls that, neither in decision-making on introduction of the new technology nor in the preparation of the relevant projects are the duties following from the Personal Data Protection Act taken into account. The reasons why personal data of the clients are being processed and retroactively incorporated in the entire information process are conceived only subsequently, and often artificially

Findings on utilisation of the RFID technology

In its supervisory activities, the Office encounters another frequent use of chip cards, particularly in entrance checks, electronic locks and control of attendance by employees. Similar to all other technologies, the properties of RFID chips are used to improve a certain activity. However, it remains a fundamental problem that the collected and subsequently processed data cannot be controlled. Contact-free technology allows the controller to install chip readers at any place, also concealed, as well as to program the entire equipment for various functions. Systems are used in practice that allow, not only for entry by the authorized card holders to a certain area, but also for recording information on the entry, i.e. identification of a certain chip and time of entry. Increasingly often, these systems are supplemented by additional chip readers, which are located, not only at entrances, but also on other internal premises. Given the fact that RFID transmitters have a range of approx. 10 meters, it is easy to detect all movements of chips in the vicinity. Thus, the fundamental problem lies in the fact that a common holder of a chip card cannot affect what data are being collected and retained through the RFID and, in particular, is unaware of the manner and reason for their processing and evaluation, because the controller is the only person to have any practical ability to check this state of affairs. Particularly in labour-law relationships, the use of the RFID technology contributes to an unequal position of the employees and the employer.

In contrast, compared to foreign countries, in its supervisory and consultancy activities, the Office encounters only rare use of the RFID technology in commerce – in the area for which this technology was originally developed – i.e. in the area of logistics and surveillance of circulation of goods, business activities, checks in dry-cleaning and laundry operations, rental shops, etc. Nevertheless, the Office monitors the development and gradual application of this technology from time to time also in this area.

However, the Office also records information on further use of the RFID technology, such as monitoring of bank notes and duty stamps or identification of animals. Special attention is being paid to utilization of the RFID technology in health care, where it serves for controls during the treatment process. The Office has not yet encountered the fashionable application of a chip under the skin, which then serves as a credit card. With the gradual decrease in the price of production of RFID chips, it can be anticipated that they will be more extensively used in every-

day life, which fact will naturally result in more frequent misuse of the properties of RFID. Contact-free exchange of information, which is almost impossible to control, and the attempts to collect information of any type for subsequent use, is a realistic threat.

UNSOLICITED COMMERCIAL COMMUNICATIONS

The subject of dissemination of commercial communications is regulated by Act No. 480/2004 Coll., on certain services of the information society, which transposes the relevant EC directives concerning the conditions of electronic communication in trade. Similar to the relevant laws in other Member State, it also raises certain interpretation questions. It can be stated that, having the experience it has obtained, the Office now very intensively fulfils the role of a regulatory authority for this area, although it continues to encounter attempts of the senders of commercial communications to find certain gaps in the Act or to take advantage of issues related to interpretation, in order for them to be able to send commercial communications to potential customers without their prior consent. Fair traders thus often become illegal senders. It can be stated in general that the number of complaints lodged with respect to sending unsolicited commercial communications remained the same as in 2007. In 2008, the Office focused, within its control and administrative activities following from the competence to punish unsolicited commercial communication, particularly on those entities that were sending commercial communications to a greater extent or that repeatedly violated the aforementioned law. The Office received 1458 instigations related to sending unsolicited commercial communication in 2008, of which it resolved 1311. 155 controls were commenced and 91 controls were completed during the year. 255 complaints were found unjustified (in 176 cases, a commercial communication was not involved and 79 came from abroad); in 94 cases, the sender was not found. A remedial measure was imposed on 320 entities. Administrative proceedings were pursued against 81 entities and fines were imposed on them, through a final decision, in a total amount of CZK 896,500.

International cooperation

The Office is involved in the European Contact Network of Spam Authorities (CNSA) and in the London Action Plan (LAP). Within these international initiatives, the individual cases can be referred to the country of origin. However, the Office only rarely receives complaints against foreign unsolicited commercial communications. Breach of the international criteria – i.e. quantity, damage or harm caused – could not be proven in respect of any of them. Act No. 480/2004 Coll., on certain services of the information society, is stricter than the laws applicable in a majority of European countries, as it does not contain the aforementioned limiting criteria. However, these criteria are taken into account in decision-making on the amount of the penalty.

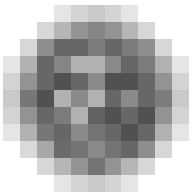
As regards cross-border enforceability of the Act, the Office proceeds pursuant to Regulation (EC) No 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation). An international information system entitled CPCS (Consumer Protection Cooperation System) has been established within this cooperation. During the year 2008, the Office obtained access to the TESTA II communication network, which allows for data exchange within the CPCSA system for

all bodies involved in the network. Thus, through this system, the Office can refer, to the competent foreign bodies, those cases that involve a foreign element (e.g. the sender of unsolicited commercial communication is established in one of the European countries).

Control process

This process is often prolonged.

In the performance of control concerned with compliance with the duties in sending commercial communications by electronic means, the Office proceeds pursuant to Act No. 552/1991 Coll., on state control. The administrative procedure related to such a complaint can be a very prolonged process in this regime. Upon commencement of control, questions, which are now standardized, are given to the controlled entity in relation to the commercial communications sent by this entity. If the relevant inspector has any doubts as to the veracity of the answers provided, he invites the controlled entity to supplement the answers or carries out control on site. The length of the control process thus depends particularly on complexity of the case and cooperation by the controlled entity. If the controlled entity does not provide the cooperation required for the control, procedural fines are imposed; the inspector has no other option and the entire control process is thus prolonged. The control process is then closed only upon expiry of the deadline for lodging objections against the control protocol or when these objections have been dealt with. If violation of the law is found, the control proceedings are followed by administrative proceedings – here, the party may use remedies, which again prolong the proceedings. The complainant is then advised only of the decision on his complaint, i.e. often only after the administrative proceedings have been closed and thus once the decision has already become final.



Supervisory and administrative activities

ACCEPTANCE OF INSTIGATIONS AND COMPLAINTS, PROVISION OF CONSULTANCY

Telephone inquiries made by citizens are primarily and generally addressed by an independent workplace established within the Department for Contacts with the Public, which frees the hands of the employees entrusted with legal assessment of the contents of written instigations and complaints for breach of the duties imposed by the Personal Data Protection Act. Only in case of more complex telephone inquiries and applications is the reply provided by an officer specializing in the relevant area, or these officers provide a written response or personal consultation. The following entities can be mentioned amongst those to which 68 personal consultations were provided by this department in the relevant year to central bodies of State administration, public administration and the private sector: Ministry of Defence, Ministry of Interior, Ministry of Justice, Ministry of Industry and Trade, Ministry of Transport, Ministry of Education, Youth and Sports, Ministry of Health, Office of the Government, Czech Telecommunication Office, Telefónica O2, Czech Mining Authority, Prague Heating Company, Prague Airport, Prague Air Navigation Services, Škoda auto, ČSAD SVT Prague (Transport Company), Czech Antidoping Committee. Based on a request for consultation, the Office usually assessed the presented projects and provided its opinion.

In spite of an increase in the number of inquiries received by the department (1 778 inquiries were answered, compared to 1 674 in the year 2007), the department was able to maintain the average time required for responding to the instigation or request at approx. 10 business days.

A total of 697 instigations for initiation of proceedings ex officio were dealt with, which corresponds to an increase by 21 % compared to 574 instigations in 2007. Practically the entire increase was reflected in the number of instigations rejected as unjustified, where it was explained and justified to the complainants in detail, often repeatedly, why the Office had found no reasons for enforcing its supervisory competence. 64 % of petitions were thus rejected as unjustified.

The Office again dealt with anonymous petitions which it, however, continued to consistently address according to the relevance of its contents, particularly where it considered the anonymous instigation received to be instigation causing a justified suspicion that an incorrect procedure of a personal data controller or processor could affect a great many data subjects and resolution of the ascertained defective state of affairs is thus an important public interest or involves an important set of sensitive personal data. These instigations are also referred for verification to inspectors of the Office.

The most frequent issues, or concerns of the citizens in the position of data subjects, continued to include, in 2008, camera surveillance systems, processing of sensitive personal data in health care, records kept by public administra-

tive bodies and local governments and introduction of various types of chip cards, particularly in transport. Given this enormous interest, these issues are the subject of separate sections of the Annual Report concerned with control activities.

The most effective method consists in systemic resolving of the ascertained shortcomings together with the relevant substantively responsible governmental and private entities. Therefore, the Office consistently engaged in negotiations with the Ministries of Justice, Health, Finance and Interior, the Association of Housing Cooperatives, the Association of Hotels and Restaurants of the Czech Republic, the Transport Company of the Capital of Prague and also the Office of the Ombudsman, which has been an important partner for the Office in the area of protection of fundamental human rights. The Office has actively participated in a conference entitled "Comprehensive Security" held by F. S. C. Bezpečnostní poradenství, a.s. within the ISET 2008 international fair. In 2008, the Office continued to strive to force the competent authorities to adopt measures aimed at changing the current legal state where the duty to enter personal data in publicly accessible lists is in conformity with the special legal regulation, but, in the opinion of the Office, is not in accord with the general principles of personal data protection. Based on an initiative of the Office, cooperation was commenced with the Ministry of Justice and the current legal state should remedy be remedied by an inter-sector expert group preparing an amendment to the Commercial Code.

With respect to the increasingly frequent cases of processing of biometric data for identification or authentication of data subjects in labour-law relationships, particularly in relation to the operation of electronic attendance control systems, the Office is preparing a new and relatively restrictive standpoint, which will be published on its website shortly.

KEEPING THE REGISTER OF PERMITTED INSTANCES OF PERSONAL DATA PROCESSING

The general public is informed of registered instances of personal data processing through a publicly accessible register posted on the website of the Office and allowing for remote access. Registration proceedings are commenced upon delivery of the registration petition, which is then evaluated from the viewpoint of the requisites stipulated by the law. If the notification lacks any of the requisites, the notifying party is sent a notice with specification of the inadequate or missing information and a deadline is set for supplementing the notification. If the deadline is not met by the notifying party, the notification is deemed not to have been lodged. Subsequently, the Office considers whether the notification indicates a justified concern of violation of the law and, thus, whether it is appropriate to commence administrative proceedings against the controller or whether there is no such justified concern and the personal data processing can be registered.

The above-described consideration is based on information provided by the controller within the supplied documentation. Thus, it is up to the controller to ensure that the alleged facts correspond to the actual facts. Furthermore, it should be noted that, in this stage, the Office considers instances of processing that are actually not yet taking place, or should not be taking place (however, the practice is different and the Office is often notified of processing that is already taking place and the controller is attempting to achieve its subsequent legalization).

An integral part of activities of the registry consists in issuing decisions on cancellation of registration. 90 instances of processing were thus cancelled during the relevant year at request of the controller, mostly for the reason of termination of the company or its merger, cessation of business activities or termination of processing of personal data. The Office publishes information on cancelled registrations in the Journal. A registration notification that does not contain any defects is entered in the register. The controller may commence processing only when the processing has been entered in the register, which fact he can ascertain by inspecting the public register, which is available on the website of the Office. In case of lack of activity of the Office, after expiry of 30 days from the date of delivery, the processing is deemed to have been registered. Only on the basis of a request shall the Office issue, to the controller, a registration certificate, which contains the date of issuance; reference number; name, surname and signature of the person who issued the certificate; imprint of an official stamp; identification details of the controller; and the purpose of processing. By means of timely registration, the controller can become aware of fundamental issues related to the intended processing and can thus avoid an unlawful procedure in personal data processing and also a potential fine for a misdemeanour or other administrative offense. 749 such proceedings were held in 2008, which is approx. 23 % of the total number of notifications received.

The effectiveness of submission of notifications through the electronic form and the website of the Office was repeatedly confirmed in 2008.

Many notifying parties 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.

If the Office comes, on the basis of the information provided by the controller during the registration proceedings, to the conclusion that the given processing is not subject to the notification duty, this fact is communicated to the notifying part by a letter, with advice that the processing has not been entered in the register and with the reasons for this procedure.. Similar to 2007, the number of registration notifications again increased in 2008.

The most frequent type of processing notified in 2008 consisted clearly in data processing via a camera surveillance system; the increase was more than two-fold compared to the previous year.

Notifications of processing of personal data and inquiries concerned with “whistleblowing” became increasingly frequent in the third quarter of 2008. It should be stated in brief that this is a system introduced by companies that originate from or are co-owned and controlled by companies established in the U.S.A. The introduction of this notification system is a duty imposed by the U.S. SOX Act (i.e. Sarbanes-Oxley Act), which is now being promoted also in the EU. The experience obtained to date indicates that this system entails primarily processing and subsequent transfer of personal data to the U.S.A., as there are currently no companies established in the territory of some other country that would provide the necessary services to companies which have introduced this system. Indeed, a new functional element of the system consists in participation of an independent and unbiased entity that is to examine notifications lodged by employees which are aimed at higher ranks in the company management.

The system then entails the processing of personal data of two categories of subjects, i.e. the notifier (whistleblower), who de facto grants consent to such processing through his petition, and of the entity that is subject to the notification, i.e. the person with respect to whom a notification of a harmful conduct is made. It can be considered on the basis of inquiries and notifications of personal

data processing received to date that the companies are aware of the existence of the WP 117 working document and, if not, they instinctively set their systems in accordance with this document. The sole issue in this respect appears to lie in unclear roles of the controller/processor in certain cases, or the manner in which the data flows occur.

TRANSFER OF PERSONAL DATA ABROAD

Applications lodged by legal persons in 2008 were concerned, similar to previous years, especially with transfers of personal data of employees or applicants for employment to parent companies abroad, particularly in the United States of America. The indicated reasons mostly consisted in activities related to common personnel policies, planning of personal development of employees, more effective use of human resources and planning of further education of employees. 148 registered controllers transferred data to the countries of the European Union in 2008. Transfer of personal data to all other countries can take place within the regime of Article 27 (2) or (3) of the Personal Data Protection Act.

In 2008, this involved mostly transfers of personal data with consent or based on an instruction of the data subject. Relatively often this included a transfer of personal data that was required for negotiations on the conclusion or amendment of a contract, taking place at the initiative of the data subject, or for the performance of a contract to which the data subject was a party. This condition was fulfilled particularly by those controllers who were active as insurance companies, travel agencies or real estate agencies.

Standard contractual clauses

In 2008, the Office assessed a case, where the controller submitted contractual clauses which he considered to be "standard" according to the Commission's decision. However, based on their assessment, it had to be concluded that the contractual clauses in the form in which they were presented to the Office could not be considered to be a sufficient instrument for transfer of personal data of employees/clients to third countries on their basis. One of the main reasons lay in the absence of liability of the data exporter or importer towards the data subject for breach of his contractual obligations and of the right of the data subject to enforce this clause, as an entitled third party, against the importer or exporter of data, should he breach his contractual obligations in relation to the personal data of the data subject. Moreover, the purposes of processing were not sufficiently described and there was no justification for the need to transfer also sensitive personal data on the data subjects, etc. Consequently, in conclusion, it had to be stated that the presented contractual clauses do not provide sufficient guarantees of personal data protection for the transfer of the personal data to third countries within the meaning of Art. 26 (2) of the Directive and Article 27 (3) (b) of the Act.

Safe Harbour (SH)

The number of controllers utilizing this instrument for transfers of personal data to the U.S.A. substantially increased during the past year. This instrument is mostly used for transfers related to employment relationships. Unfortunately, similar to standard contractual clauses, the Office is not sufficiently aware of the actual functioning of this instrument in practice in terms of the manner and sufficient scope from the viewpoint of the Act and the Directive.

Binding Corporate Rules (BCR)

During the past year, the Office encountered several cases of BCR that were submitted to it for assessment. In all cases, the leading data protection authority came from another EU country. The Office has not yet been asked to act as the leading DPA. In its assessment of the BCR, the Office attempts to approach the rules from a more conceptual and principal viewpoint, i.e. concentrates on the internal logic of the BCR, and deals with the contents particularly in terms of determining as to whether the BCR contain all the necessary principles and elements they should have. In its response, it then always emphasizes that this assessment is only preliminary and that authorization of the Office pursuant to Article 27 (4) of the Act will have to be applied for in case of an intention to transfer personal data on their basis from the Czech Republic to third countries. The response also points out particularly that, for the reasons of national differences in various areas of legislation, especially in the area of labour law, the BCR will have to be correspondingly adapted to the national legislation, which could also be done with assistance of the Office after submission of the application pursuant to Article 27 (4) of the Act.

PERFORMANCE OF ADMINISTRATIVE ACTIVITIES OF THE OFFICE

Administrative proceedings are pursued both by inspectors of the Office and by the Section of Supervising Activities. The agenda of the section is concerned not only with proceedings pursuant to the Personal Data Protection Act, but also with all proceedings that are pursued by the Office pursuant to special laws. These laws include, in particular, Act No. 133/2000 Coll., on register of population and birth numbers and on amendment to some laws (Register of Population Act), and Act No. 159/2006 Coll., on conflicts of interests. Furthermore, the section holds proceedings pursuant to Article 17 of the Personal Data Protection Act in cases of justified concerns about the legality of processing notified to the Office. These activities of the section also involve methodical unification of the procedures of the Office within the scope of the Code of Administrative Procedure.

The performance of the Office's powers in the area of administrative punishment can be classified, on the one hand, according to the laws that stipulate the powers of the Office to discuss administrative offenses (misdemeanours and other administrative offenses of legal persons and natural persons operating a business) and, on the other hand, according to the authors of the instigations received by the Office for discussion. In the area of misdemeanour proceedings pursued for a suspicion of violation of the Personal Data Protection Act, 60 % of instigations are lodged by the Police of the Czech Republic or other public administrative authorities and local governments (misdemeanour committees), while the remaining cases are discussed on the basis of information from private persons (usually natural persons) who have directly addressed the Office. With respect to discussion of other administrative offenses pursuant to the Personal Data Protection Act and the Register of Population Act, only 20 % of the instigations are lodged by public administrative authorities, while 35 % of the instigations result from control findings of the inspectors of the Office and the highest share (45 %) are instigations from private persons.

The instigations sent to the Office by the Police of the Czech Republic are most frequently concerned with a suspicion of inadequate securing of the processed data against their unauthorized processing, because some documents (preferably contracts, but even healthcare documentation) are found in waste bins, collection

yards or thrown out in a forest. Thus, these cases involve active conduct of persons who leave the documents at such a place, whether they are individual employees or even the persons responsible for processing in the position of controller or processor themselves. The second group of cases involves negligent conduct of the mentioned persons, who leave documents containing personal data, e.g., in an unlocked vehicle from which they are later stolen. In this respect, it must be noted that performance of the duty to adopt adequate measures aimed to prevent risk of unauthorized processing or use of personal data requires that the responsible person duly consider all the risks associated with the personal data processing undertaken by this person and adopt the corresponding measures to eliminate such risks. Indeed, an administrative offense is committed even in case of occurrence of a certain threat to personal data, although they have not yet been processed without authorization or this even never occurs. This duty is based on strict liability for its breach; i.e. only if the controller or processor, as appropriate, demonstrates that he exerted all efforts that could be requested to prevent the breach of the legal duty, he is not liable for the administrative offense.

Imposed penalties

A fine of CZK 100,000 was imposed during the relevant year on a State-owned company that failed to ensure that the recording of a telephone conversation between its operator and Mr. I. K., which was subsequently played by radios and is freely available on the Internet, is not disclosed to unauthorized persons and also failed to inform Mr. I. K. of the acquisition of the recording. One of the highest fines in 2008 was imposed on a company that published, on its website, in relation to the provision of loans, data pertaining to 52 debtors, within the scope of their name, surname, residence address and birth number. The provider of loans in this case collected and processed personal data for the purposes of providing loans to natural and legal persons. However, it did not have the consent of these persons – data subjects – to publish their personal data on the Internet, where they were made available to a large number of people. Indeed, publication of the personal data of debtors must be considered to be a means of exerting pressure that also breaches other provisions of Article 10 of the Charter of Fundamental Rights and Freedoms. Because an appeal against the decision of the first-instance administrative body was lodged late, the President of the Office rejected it and the decision came into legal force. Another penalty was imposed by the Office on a company that published, in relation to organization of public auctions, at least in two cases, an annex to an auction notice containing a list of employees of the applicant for the auction, including personal data within the scope of the surname, name, date of birth, date of commencement of employment, amount of the salary tariff, % bonuses and the total amount of the salary, all this without consent of the affected employees. This resulted in processing of personal data with a scope exceeding the purpose for which they were collected, for which a fine was imposed on the company in the amount of CZK 25,000. The decision of the first-instance administrative body was contested by an appeal, which was rejected by the President of the Office and the decision thus came into legal force.

Proceedings pursuant to Article 17 of the Personal Data Protection Act

Proceedings pursuant to Article 17 of the Personal Data Protection Act follow the procedure in the performance of the notification duty pursuant to Article 16 of the Act. In cases where doubts regarding legality of the notified processing are not eliminated even through an invitation to supplement the notification, the responsible

organizational unit (Division of Registration) refers the file for administrative proceedings to the Department of Administrative Activities. These proceedings aim to eliminate a justified concern that the processing could result in violation of the law, although it follows from the wording of the law that the Office could make a decision on rejecting the processing in case of any unlawfulness. Oral negotiations are primarily pursued to this end, where the main duties in personal data processing and the conditions under which the processing can be carried out are explained to the controller. During the entire administrative proceedings, the controller can freely change the parameters of the notified processing. Indeed, such changes are mostly a reason why the justified concern of unlawfulness of processing ceases to exist and the proceedings are later discontinued and the notified processing is (as changed) entered in the register of processing.

In general, the results of this type of administrative proceedings can be summarized in that approx. 80 % of the pursued proceedings are discontinued as there is no longer any justified concern of breach of the conditions stipulated by the law; in 10 % of cases, the processing is not permitted and the remaining 10 % of proceedings are discontinued for procedural reasons, such as withdrawal of the notification of processing by the party, etc.

Number of proceedings held:

Administrative punishment (proceedings pursued by the Department of Administrative Activities)

– administrative proceedings for violation of Acts Nos. 101 and 133 ------ 54
– misdemeanour proceedings for violation of Acts Nos. 101 and 133 ------- 8
– misdemeanour proceedings for violation of the Conflict of Interests Act ---- 0

proceedings pursuant to Article 17;

of which:

– discontinued (the data controller is not in breach of the conditions stipulated by the Act) ---------- 78
– discontinued for procedural reasons (e.g. notification withdrawn or no personal data processing) ---------- 9
– not permitted ---------- 12

PERFORMANCE OF LEGAL REVIEW

The activities of the Office in the area of review of administrative decisions are concentrated within the Department of Legal Support and Schengen Cooperation (DLS), which is involved particularly in decision-making of second instance in all cases where a remedy is lodged against a legal act of the Office and where a decision is to be made by the President of the Office. This involves specifically decision-making on appeals lodged against a decision on imposing a penalty for violation of the law, within which the Office is entrusted with supervision (or decision pursuant to Article 17 of the Personal Data Protection Act), or decision-making on objections lodged against the control protocol drawn up by an inspector of the Office. In these cases, the DLS prepares basic documents for meetings of the appellate committee of the President of the Office, or the board of inspectors, and subsequently also the final decision in the case. Further tasks of the DLS include the preparation of materials requested by the courts after an action has been lodged against a decision of the Office.

An entirely separate area consists in the fulfilment of the tasks following for the Office from its position of authority authorized to supervise personal data protection in the field of the Schengen cooperation, i.e. particularly data processing with-

in the national part of the Schengen Information System (SIS). In this respect, the mentioned department provides for the participation of the Office in meetings of the joint supervisory body entrusted with the control of the central part of the SIS and unification of the approaches of the national authorities, and also contributes to the performance of control of personal data processing by the competent authorities in the Czech Republic. The DLS performs a similar activity also in the related area of personal data processing within the EURODAC system or in the Customs Information System.

Second-instance administrative proceedings

– 16 meetings of the appellate committee took place in 2008 (including once "per rollam")
– 36 cases were discussed
– total number of appeals lodged: 33 (of which 4 pursuant to Article 17)
– final decisions: 21
– 12 meetings of the board for discussing objections took place in 2008
– 21 cases were discussed
– total number of objections lodged against the CP: 25
– final decisions: 20 (including objections against destruction)

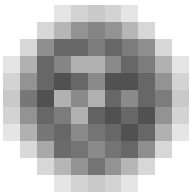
Court proceedings initiated by an action against a decision of the Office

Total number of court proceedings in 2008: 13

Year	Total number of actions	Proceedings at the Municipal Court in Prague	Proceedings at the Supreme Administrative Court (cassation appeal)	Constitutional Court	Actions terminated	Actions pending
2001	1	–	–	–	1	0
2002	2	–	–	–	2	0
2003	1	–	–	–	1	0
2004	3	–	–	–	3	0
2005	8	2	3	–	3	5
2006	7	4	2	–	1	6
2007	12	9	1	–	2	10
2008	13	12	–	–	1	12

Aspects of judicial review

Similar to an ordinary remedy aimed against legal acts of the Office (i.e. objections against the control protocol and appeal against a decision issued in administrative proceedings), it is not uncommon in the practice of the Office that an action is lodged with an administrative court; on the contrary, this remedy is used in a great many cases and increasingly often. For illustration, it can be stated that, in 2008, 11 actions were lodged against a decision or control protocol of the Office; while this number is similar to the number in 2007, it is two-fold compared to 2005 and 2006. Similarly, as in other areas of activities of the Office, the actions are concerned with ever more complicated aspects of interpretation and application of legal rules, where the response is awaited not only by the plaintiff (mostly the personal data controller or processor on whom the Office imposed a fine), but also by the Office itself, because, in certain cases, the court decision can have a substantial impact on the practice of the Office.



Legislative activities

Undoubtedly, the most important planned change in the legislation of the Czech Republic was related, in 2008, to the preparation of the new codification of civil law and work on new electronic registers of public administration.

With respect to **electronisation of State administration** and introduction of e-government services, it is clear that this is not only a complex technical issue, but also, to a greater degree, a social problem. This problem is not resolved once the legislation is prepared and the relevant computer applications launched, but also requires awareness raising and improvement in user capabilities of the citizens and officers, at least concurrently with the legislative process.

With respect to a system that will play a key role in the near future in the area of e-government in the Czech Republic – the system of data boxes – the period of maintaining data in the new records was substantially shortened on the basis of a comment raised by the Office. Furthermore, the Office questioned a proposal for a new electronic identifier for citizens – personal number – which is related to the existence of data boxes to a certain degree. Indeed, this identifier was proposed in a rather unclear form, but with an ever clearer intention – that it be used, in the future, for other purposes pursuant to other laws (the proposal was later considerably narrowed to a mere number of the data box). From the viewpoint of the principles of due personal data processing, it is also important that electronic communication and acquisition of a data box will be ensured for the citizen once this is actually required (rather than obligatorily, or from birth, as originally proposed).

The preparation of new electronic (basic) State registers was not completed in 2008 from the legislative viewpoint. The Office strived to contribute in this respect particularly through its consultancy activities, with emphasis on summarizing the foreign experience and on the importance of the function of safe electronic identifiers that would be different for the individual agendas (this is one of the principles of e-government). In this respect, the Office referred to the drawbacks of the existing State registers which do not have uniform security guarantees, which are mutually interconnected and, from the viewpoint of personal data protection, can also be more easily misused. The Office anticipates that the general duties concerning personal data protection will also apply in activities concerning new electronic registers and, consequently, this area will be subject to supervision by the Office.

Within provision of comments on the draft new Civil Code, the Office criticized the regulation of acquisition of records and recordings by technical means, which is highly inadequate in terms of the modern trends in automated personal data processing. After consulting the Office, the Ministry of Justice pledged to modify the draft so that it more clearly expressed the preconditions for acquiring images and records and recordings of conduct of persons, particularly on public premises and other places accessible to the public. In this respect, account may be taken of the results of two materials concerning the legal regulation of camera surveillance systems, to which the Office contributed in 2008 and which are being prepared within an MPs' initiative and also within the committees of the Government Council for Human Rights.

The Office considers it positive that the draft Civil Code has been reformulated in the part concerning identification of citizens. This Code, which is based on the principles of natural law, should emphasize and, in a certain way, summarize all the positive approaches to date, including identification stipulated in the field of justice particularly in procedural regulations and based on utilization of natural identification details of a person, such as his name, surname, birth details or address of residence.

The creation of a draft new Commercial Code is also related to the aforementioned Civil Code. The Office opposed to adoption of the current provisions of the Commercial Code, where the rules for publication of personal data are defined very ambiguously and, moreover, by a secondary regulation. The Office welcomes the pledge for a separate law on the Commercial Register made by the Ministry of Justice, where it will be possible to discuss in detail the rules concerning particularly electronic processing of data in the Register and their publication on the Internet.

During the entire year, public interest was drawn by the preparation of the **law on census of population, buildings and apartments** in 2011. In this respect, the Office concentrated its comments on ensuring that, also in the newly planned electronic census, as well as within the work of the census officers and potential cooperation with external entities, there are clear rules for accessing certain information and that data are secured against misuse. It has shown that a substantial issue was related to the manner of retaining data after completion of the census, in a not entirely anonymous form. The existence of a set of data, originating not only from the planned census, and potentially supplemented from other records, and without a more specific regulation in another important law, the Act on the State Statistical Service, was ultimately left for discussion at the level of the Government, which omitted the proposed provisions on the set of data from the Act.

The subject of new regulations concerning **healthcare registers** is currently, in the opinion of the Office, underestimated in society; in this area, the Ministry of Health did not accept the requirement of the Office for full clarification of the concept of the registers. The Office requested explanation of the justification of the set period of retention of data in the individual registers, as well as explanation why the registers fail to take account of the consent of the affected persons, as is common in other European countries. Indeed, the Office recommended that, in the interest of maintaining the standards of protection of highly sensitive data maintained in the registers, the indicated aspects of the registers be regulated by a law, rather than by a ministerial decree or an annex to a legal regulation.

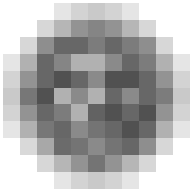
In relation to the Personal Data Protection Act, certain questions concerning the supervisory competence of the Office were also raised due to some legislative approaches that had not been coordinated with the Office. In addition to the usual attempts to exclude personal data protection from the legal system by stipulating or assuming, in the draft legal regulation, that certain information concerning an individual does not constitute personal data (this is a clear variance with the broad definition of personal data in the Personal Data Protection Act and also in the relevant EU Directive), there were certain more or less unintentional attempts to subject the supervisory competence of the Office to certain exemptions from confidentiality pursuant to special laws. However, a special regulation in this respect is redundant as the authorization to work with any protected personal data that are to be controlled from the viewpoint of performance of duties in personal data processing is granted to the relevant inspectors and other control workers directly by the Personal Data Protection Act. The above is based on the EU Directive, which also served as a basis in the creation of the competence and procedural provisions of the Personal Data Protection Act. Therefore, the Office welcomed that

the Euro-conforming construction was also confirmed by the Ministry of Finance in relation to the supervision by the Office over personal data processing pursuant to the Act on Selected Measures Against Legitimisation of Proceeds of Crime and Financing of Terrorism.

In 2008, the Parliament discussed an MPs' draft amendment (see parliamentary print No. V/171/0) to the **Conflict of Interests Act**, which was highly questionable from the viewpoint of personal data protection. In respect of the amendment, the Office maintained its position that the draft amendment was rather a cosmetic modification which did not resolve substantial defects of the Conflict of Interests Act. Therefore, in February, the Office addressed the Constitutional Law Committee of the Chamber of Deputies of the Parliament and the Standing Commission of the Senate for Privacy Protection with a request for supplementation of the draft. However, this did not occur, because the Senate rejected the draft amendment. Nevertheless, ultimately, the amendment came into force and effect without any substantial changes in the form of Act No. 216/2008 Coll. It is a mistake that the Conflict of Interests Act fails to unambiguously distinguish between constitutional and other elected officials, whose privacy is often substantially less guaranteed given their public position, and public officers, where the protection of privacy must be, in principle, maintained, unless their official activity is at hand. Furthermore, the character of the law is further magnified by the manner of disclosing personal data concerning the assets and financial liabilities of the affected persons, where it is not always clear as to whether and, if so, how it will serve to detect a potential conflict of interests. During legislative work, the Office simultaneously provided consultancy concerning the manner of performance of duties pursuant to this Act, so that further infringement of privacy of the affected persons would be avoided if possible.

The Conflict of Interests Act, similar to other legal regulations, often attests to the lack of preparedness of the authors of the laws to take account of new technologies and trends in personal data processing, particularly with respect to disclosure and publishing personal data. In relation to the proposal for basic registers, the Ministry of Interior finally proposed to supplement the function of keeping register of population by the possibility of providing people, under certain preconditions, with a contact of the sought person, i.e. a function that was proposed by the Office already five years ago. The regulation of use of internet in the legislation is often absolutely misconceived. Numerous persons responsible for personal data processing are not aware that publication is also a form of personal data processing pursuant to the law, where it is necessary to take account of all the relevant principles of data protection. Instead of utilizing or, on the contrary, prohibiting browsing, sorting and access functions of the program equipment of the internet network, personal data are published in the given lists extensively, without any further measures that would normally be taken in case of manual processing of data and that must also be adopted in electronic form (cf. Article 13 of the Personal Data Protection Act). The regulation of provision of information in the practice employed by municipalities, where the data are still being rendered anonymous, can serve as an example in this respect, as it is clear that extensive publication on the internet makes data accessible also to those users of the internet to whom provision of personal data discussed within the municipal order is neither purposeful nor legal. Preferably, the submitting party refers the case to further discussion on the basis of a comment raised by the Office (as in the case of the Commercial Code); in the worst case, it rather gives up on the idea of amending the regulation, as occurred in late 2008 with respect to the set of amendments to the election laws (amongst other things, the Office requested that it be clarified as to what would be published on the internet and for what reason).

In spite of its limited capacities, in 2008, the Office strived to monitor the creation of legal regulations in all areas providing for personal data processing. Unfortunately, not even a governmental system of electronic comments on documents ensures that the Office, which is not an obligatory commentary place pursuant to the Legislative Rules of the Government, learns of preparation of materials dealing with processing of information on individuals in due time. Therefore, the Office considers it more suitable to be addressed, in due time, by the responsible ministries to which it offers, in the preparation of concepts, analyses and substantive intentions, consultations on impacts on protection of privacy and evaluation of changes with respect to the rules of the Personal Data Protection Act, as was the case in 2008, e.g., in relation to amendments to the Act on Free Access to Information or the newly prepared Act on Control.



Relations to foreign countries and international cooperation

Cooperation with the EU bodies and partners in the EU Member States is a clear priority within relations of the Office with foreign countries.

An important role in the activities of the Office in relation to cooperation with the European Union was played by **preparations for the Czech Presidency of the Council**. Within the commentary procedures, which took place in several steps, the Office put forth its standpoints and opinions in the creation of two basic program documents that were drawn up by the Government of the Czech Republic for the needs of the Czech Presidency of the Council: "Eighteen-month program of French, Czech and Swedish Presidencies" and "Substantive priorities of the Czech Presidency of the EU Council in the 1st half of 2009".

The main objective of participation of the Office in the preparation of these documents was to point out the aspects of personal data protection and to organically incorporate the relevant provisions in the planned activities.

This intention and the related ideas suggested by the Office had little success. The authors of the materials were clearly unwilling to "complicate" the topics intended to be promoted during the Presidency by aspects of human rights.

At the end of the year, intensive preparations were carried out for three important events organized or co-organized by the Office in March 2009:

(1) The Case Handling Workshop: This is a regular meeting of professionals from partner data protection authorities throughout Europe. Based on invitation from the Office, the meeting took place this time in Prague, from March 12 to 13, 2009. The program was focused particularly on the most topical issues – e.g. camera surveillance systems, biometrics, data processing in the area of employment or the subject of privacy protection in the media.

(2) Czech-French meeting of top representatives of the Office for Personal Data Protection and the CNIL – Commission Nationale de l'Informatique et des Lib-

ertés, a French independent supervisory authority. The meeting took place with support of the French Institute in Prague on March 3 and 4, 2009.

(3) A meeting of the Data Protection Working Party (G.09) took place in Brussels on March 23, 2009.

The most important working platform for relations and cooperation with both the European Commission and the partner supervisory bodies in other EU countries, again consisted, during the previous year, in the **Data Protection Working Party established under Article 29 of Directive 95/46/EC (WP 29)**.

The Office continued to actively participate in the **Joint Supervisory Body of Europol (JSB)** in 2008. A representative of the Office, inspector PhDr. Miroslava Matoušová, acted as the coordinator of the control team which carried out a regular control of personal data processing by Europol at the seat of this body in March 2008 and, until October 26, 2008, she had been the Vice-Chairwoman of this body.

The Office also participated in the work of the unusually active **Working Party on Police and Justice**. A mention should be made of an important initiative of the representatives of the Office in the Joint Supervisory Authority for the Schengen Information System (JSA Schengen), the Joint Supervisory Authority for the Customs Information System (JSA Customs) and the EURODAC Supervision Coordination Group.

Joint activities of representatives of the supervisory bodies in the area of data protection from the countries of Central and Eastern Europe and Baltic countries, which were commenced in 2001 on the basis of an initiative of the Czech Office and the Polish Office of the General Inspector for Personal Data Protection, also continued in 2008. These activities take the form of working meetings and other contacts, including communication through the common website (www.ceecprivacy.org). A declaration to support further strengthening of the cooperation of the participating countries and a declaration on equal approach to all national languages of the EU Member States (with emphasis on the practice in WP29) were adopted at the last meeting.

Contacts with the Polish Inspector General for Personal Data Protection and the Slovak Office for Personal Data Protection were above-standard and especially beneficial. In relation to the project of assistance to Bosnia and Herzegovina completed in 2007, contacts were renewed with the newly established Data Protection Commission in Sarajevo.

For a number of years, the Office was represented in the project group on data protection (CJ-PD) of the Council of Europe and was also an elected member of the coordination committee (CJ-PD/CG). The Office continued to actively participate in the Data Protection Committee established pursuant to Convention No. 108 (T-PD), which is the supreme body of the **Council of Europe** dealing with data protection. The Office is represented in the seven-member steering bureau of the Committee by PhDr. Hana Štěpánková, the Office's spokesperson.

The very beneficial cooperation with the **OECD** – Organisation for Economic Cooperation and Development – has continued; in this respect, the Ministry of Interior is the partner of the Office for representation of the Czech Republic in the Working Party on Information Security and Privacy (WPISP).

Communication with the media and dissemination of knowledge on personal data protection

Press conferences

The well-established method of communication with the media continued to be employed in 2008: The popular quarterly frequency of balancing press conferences usually attracts about 20 journalists to the Office, including printed media – both dailies and professional journals – agencies and major radio and TV stations. The outputs of the press conferences were then regularly presented, during the year, only during the noon newscast on the day of the press conference. Furthermore, 30 to 60 outputs are dedicated to personal data protection over the subsequent 3 days.

Press releases and annexes to them are permanently published on the website of the Office immediately after the end of the conference.

On January 28, the Office organizes a special press conference on the occasion of the Personal Data Protection Day.

A competition for children and youth entitled "My privacy! Don't look, don't poke about! " was announced for the second time on this occasion; further details on this competition are provided below.

Contacts with the media

The media tendency to simplify matters led in some cases, particularly in case of telephone contacts, to distortion of the legal substance of the case. A similar problem can be encountered in television newscasts, where the responses are not subsequently presented to the Office for its statement and, consequently, the general public obtains one-sided information. During 2008, the Office also encountered a voluntaristic approach to a case which drew attention in the media, where the journalist adopted a pre-determined position. Unfortunately, understanding of the legal substance of the issue cannot be enforced.

In contrast, it can be considered positive that the journalists are interested in specific situations where they believe that privacy could be threatened. Very often, based on a contact of a journalist with the Press Division, the Office becomes aware of an incident that it should deal with – and, based on such notice, the case also often becomes the subject of supervisory or even control activities of the Office.

Electronic communications

The fact that the National Library has included the website of the Office in the newly created archive of those websites that are considered to belong to the national heritage is a great honour and pleasure for the Office. The website of the Office was supplemented in 2008 by an information bulletin that provides information on personal data protection and legislation related to privacy protection in countries that develop this aspect of human rights protection.

Library of the Office

The library provides a professional background for employees of the Office. In 2008, it was extended by 135 publications. It also continued to serve as a background for students of law and administrative schools. 6 students of universities and secondary schools used its resources for their theses.

Dissemination of knowledge on personal data protection

A list of all lectures on personal data protection provided in 2008 with contribution of the professional employees of the Office would be very extensive. Therefore, it will be more suitable to state that the personnel of the Office provided 260 hours of lectures in 2008.

A program prepared by the Office for teachers, which was accredited for a period of 3 years by the Ministry of Education, Youth and Sports of the Czech Republic, continued in 2008. The Office provided workshops in individual regions. These workshops took place in Hodonín, Pardubice and Ostrava. In conclusion of the workshops, the participants obtained a certificate of participation in the module "Personal Data Protection in Education" and could test their knowledge in an anonymous test. The test will serve the Office as a feedback on its ability to comprehensibly provide knowledge in the area of personal data protection.

In 2008, the Office organized the second year of a literary and artistic competition for children and youth entitled "My privacy! Don't look, don't poke about! ". The competition was successfully attended in 2008 also by children from SOS villages in the Czech Republic, the Ukraine, Kazakhstan, Russia and Bosnia and Herzegovina. The Office highly welcomes the cooperation with the Association of SOS Villages. It considers it necessary that also children who grow up outside a complete family be adequately informed of the rights that they will have as fully-fledged members of society.

The International Film Festival for Children and Youth in Zlín was again a partner of the competition. Cooperation in the form of participation in children's programs was provided by Czech Radio Prague and information for children was also provided by the MF DNES portal entitled Alík.

In relation to the success attained last year, when the competition and workshop for teachers won, for the Office, the European prize for the best public service in the area of personal data protection awarded in Madrid in 2007, the works of Czech children from the first year of the competition were exhibited in the entrance hall of the Palace of Europe in Strasbourg on the occasion of announcement of the Personal Data Protection Day in 2008.

In November, the Office provided a lecture in a workshop organized by the 3rd Faculty of Medicine of Charles University for seniors, where special attention was paid to the impact on the lives of this generation.

Personnel of the Office

96 positions were approved in the State budget for 2008, of which one position was intended for the performance of tasks following from the Czech Presidency of the EU Council in 2009.

As of January 1, 2008, the Office had 92 employees.

63 % of employees of the Office have university education. The Office allows its employees to improve their qualifications and also provides for their extension. It allows and provides language courses in the English, French and German languages.

As of December 31, 2008, the Office for Personal Data Protection had 92 employees.

Economic management of the Office

The budget of the Office was approved by Act No. 360/2007 Coll., on the State budget of the Czech Republic for 2008.

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

in thousand CZK

Summary indicators

Total income	1 642,48
Total expenditures	88 293,01

Specific indicators - income

Total non-tax and capital income and accepted transfers	1 642,48

Specific indicators - expenditures

Expenditures for the performance of tasks of the OPDP	88 293,01
of which: expenditures related to the Czech Presidency of the EU Council	2 159,76
other expenditures for the performance of tasks of the OPDP	86 133,25
Cross-cutting expenditure indicators	
Salaries of employees and other payments for performed work	40 527,82
Mandatory insurance premiums paid by the employer *)	14 207,98
Contribution to the Cultural and Social Needs Fund	765,72
Salaries of employees within an employment relationship	29 341,72
Salaries of employees derived from salaries of constitutional officials	8 979,10

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