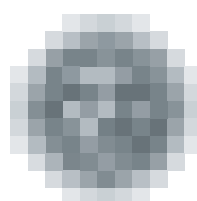


# ANNUAL REPORT SUMMARY

# 2010



**úřad pro ochranu  
osobních údajů**  
the office for personal  
data protection



# The President of the Office looks back at 2010



2010 was an important year for the Office both in view of the international recognition that it received by organising the pan-European Conference of European Data Protection and Privacy Commissioners and also in commencing the second decade of its work, through which it has been advocating the fundamental human right to the protection of privacy in the Czech Republic.

There is not much time for the Office to stop and look back; to the contrary, the pace of its work is always set by the new tasks it has to face. Nevertheless, after careful consideration, we chose a motto for the aforementioned international conference, the slogan “Weighing up the Past, Thinking of the Future”.

The present annual report naturally serves as a sort of evaluation of the past year; however, a detailed overview of the Office’s supervisory activities, its administrative decision-making and contributions to the legislative process, and the scope and contents of the received complaints also draw attention to those aspects that will have to be examined in the future. Indeed, the work of the Office is extensive and the reader of this report will surely create his own impression. Nevertheless, I would like to emphasise a few aspects.

In last year’s report, I noted that awareness and knowledge of the Personal Data Protection Act had clearly improved. However, as a consequence, on the one hand, there have been an increasing number of inquiries by citizens and, on the other hand, institutions, companies and organisations are not only familiar with the Personal Data Protection Act, but apply it with much more skill. In respect of complaints, this means that the Office must focus its consultancy activities exclusively on the competence stipulated for it by the Personal Data Protection Act and, where inquiries fall outside of this competence, it must refer citizens to other relevant legal rules. Indeed, it is clear that the increasing number of complaints and scope of consultancy cannot be handled in any other way, both

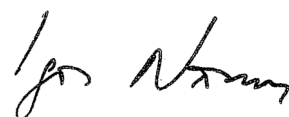
in terms of time and personnel required. In connection with the aforementioned application of the Personal Data Protection Act, we have become aware of the increasingly urgent issue of the social responsibility of institutions and companies, particularly where they require consent to the processing of the personal data of data subjects.

This issue will undoubtedly be dealt with in the context of a number of Czech legal rules on which the Office commented last year; however, our legislators have also been presented with further important bills on which the Office will comment in terms of personal data protection. Its decision-making will surely also be influenced by fundamental international legislation – Directive 95/46/EC of the European Parliament and of the Council and Council of Europe Convention No. 108 – which is currently undergoing an amendment process with active participation by the Czech Office. In this respect, I can provide information directly from the source, given that last year I was elected to the position of the Vice-Chairman of the Commission’s advisory panel for personal data protection, the WP 29 working group.

Dissemination of knowledge on personal data protection has been and will remain the centre of our attention – traditionally, this is done among the young generation; however, based on experience obtained in 2010, we shall also co-operate with various institutions, as described in the following text.

I would like to highlight one more thing. Based on the details and individual experience which are part of the annual report for the preceding year, we can foresee further trends in personal data protection, which is an aspect that continues to be an indicator of the quality of developed democracies. And unless there is a fundamental change in the paradigm of the civilisation where privacy is a fundamental value and indicator of the freedom of each citizen, personal data protection will continue to develop so as to be able to reflect, from the legal viewpoint, new technologies and technical instruments that should serve citizens without becoming their Gods and governing their lives.

The Czech Office will also contribute to this development. I have no doubt about this, because I am aware of the qualities of our employees and of the atmosphere in which we work. In this sense, I must repeat what I have already stated several times: We are a team. This fact in no way changed when we were joined by two new inspectors, who filled the positions of those whose ten-year mandate had elapsed. I am looking forward to the next year with confidence that there will be no change in the positive climate in the Office upon election of another five inspectors, who will be appointed next year by the Czech Senate and President.



Igor Nemeč



# CONTENTS

OFFICE IN NUMBERS – 2010	7
INVESTIGATION ACTIVITIES OF THE OFFICE	10
■ 2010 INVESTIGATION PLAN	10
I. General topics for specification of supervisory activities of inspectors of the Office	10
1. Public administration information systems	10
2. Information systems in the area of private law	10
3. Information systems in the area of justice	10
4. Compliance with conditions in transfer of personal data to third countries	11
5. Protection of personal data of data subjects in crisis situations	11
II. Planned activities and completed investigations following from the 2010 control plan	11
1. Investigation at the Regional State Attorney's Office in Hradec Králové	11
2. Investigation at the Hradec Králové Region	11
3. Investigation into processing of personal data of hotel guests	12
4. Investigation into personal data processing in the information systems of the Prague Social Security Administration	13
III. Investigation and supervisory activities in 2010 – conditions and general conclusions	13
■ FINDINGS OBTAINED BY INSPECTORS IN CONTROL ACTIVITIES	15
Personal data in health care	15
Opencard	16
Student registers, publication of data of university students	16
Student register	18
E-mail box contents	18
Personal data processing through camera surveillance systems	19

Non-banking entities	21
Investigation at an association of apartment owners	22
Application of the Personal Data Protection Act in cynology	22
<b>Unsolicited commercial communications</b>	<b>23</b>
<b>■ ADDRESSING COMPLAINTS AND PROVISION OF CONSULTATIONS</b>	<b>25</b>
<b>■ FINDINGS OBTAINED IN ADMINISTRATIVE PROCEEDINGS</b>	<b>25</b>
Nature of proceedings pursuant to Article 17 of the Personal Data Protection Act	25
A few comments on the term “personal data”	27
A few comments on the duty to process only accurate data	27
Personal data processing in relation to refund of credit from a pre-paid phone card	28
Street View	29
<b>■ REGISTRATION</b>	<b>31</b>
<b>■ TRANSFER OF PERSONAL DATA ABROAD</b>	<b>31</b>
<b>LEGISLATIVE ACTIVITIES</b>	<b>33</b>
<b>RELATIONS TO FOREIGN COUNTRIES AND INTERNATIONAL CO-OPERATION</b>	<b>36</b>
<b>THE OFFICE, MEDIA AND MEANS OF COMMUNICATION</b>	<b>39</b>
Website of the Office	39
Library and publications of the Office	40
<b>ORG INFORMATION SYSTEM</b>	<b>41</b>
<b>STAFF</b>	<b>42</b>
<b>ECONOMIC MANAGEMENT OF THE OFFICE</b>	<b>43</b>
<b>PROVISION OF INFORMATION PURSUANT TO ACT NO. 106/1999 COLL., ON FREE ACCESS TO INFORMATION</b>	<b>44</b>

# OFFICE IN NUMBERS – 2010

<b>Inquiries and consultations</b>	inquiries in the Czech Republic	2 451
	abroad	91
	consultations	
	for state administration	75
	for local governments	142
	for legal persons	317
	for natural persons operating a business	219
	for natural persons	1 371
<b>Pleadings and complaints</b>	instigations received pursuant to the Personal Data Protection Act	1 039
	complaints submitted for investigation	161
<b>Unsolicited commercial communications</b> (competence pursuant to Act No. 480/2004 Coll.)	total instigations	2 834
	instigations resolved	1 525
	investigations initiated	163
	investigations completed	144
	administrative decisions on a fine	96
<b>Inspections</b> (excluding controls concerning Act No. 480/2004 Coll.)	initiated	106
	completed	106
	referred to other governmental authorities	2
	challenged by objections	17
	objections accepted	0
	objections dismissed	8
	mostly accepted	3
mostly dismissed	5	
<b>Administrative punishment</b> ( <i>N.B.: *of which in respect of Article 17)</i> )	administrative proceedings for violation of Acts No. 101/2000 Coll. and No. 133/2000 Coll.	113
	misdemeanour proceedings pursuant to Act No. 101/2000 Coll.	38
	administrative and misdemeanour proceedings pursuant to Act No. 101/2000 Coll. – Article 44a, Article 45a	5
	misdemeanour proceedings for violation of Act No. 159/2006 Coll., on conflict of interests	0
	appealed decisions on violation of law	46 (2*)
	appeals dismissed	23
	cancelled and returned for new hearing	9
	cancelled decisions and proceedings discontinued	6
	change in the decision	7

<b>Judicial review</b> <i>(N.B.: **in total since 2001)</i>	court actions lodged	18 (81**)
	actions dismissed by the court	7
	decisions cancelled by the court	6
	referred for a decision (pursuant to Article 21 of Act No. 101/2000 Coll.)	0
	court proceedings closed / pending	3/15 (39/42**)
<b>Registration</b>	notifications received (pursuant to Article 16 of Act No. 101/2000 Coll.)	4 037
	instances of processing registered	3 576
	still pending	742
	registrations cancelled	119
	notifications on a change in the processing	906
	proceedings pursuant to Article 17	64
	discontinued (no violation)	55
	discontinued for procedural reasons (e.g. notifications withdrawn)	6
	not permitted	3
	<b>Authorizations for transfers of personal data abroad</b>	applications for transfer of personal data abroad received (pursuant to Article 27 of Act No. 101/2000 Coll.)
decisions on authorisation of transfers		18
decisions on dismissal		0
proceedings discontinued for procedural reasons		2
<b>Complaints pursuant to Article 175 of the Code of Administrative Procedure</b>	complaints received	34
	complaints found justified	5
	complaints found partly justified	3
	complaints found unjustified	25
<b>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</b>	instigations received	0
	instigations found justified	
	instigations found unjustified	
<b>Applications pursuant to Act No. 106/1999 Coll.</b>	applications received	20
	applications resolved	15
	applications rejected	4
<b>Materials published</b>	Journal of the Office (number of volumes)	3
	Bulletin of the Office (number of volumes)	1



Press conferences	regular	2
	extraordinary	0
Legislative drafts on which comments were made	laws	59
	implementing regulations	0
	draft Government regulations	21
	draft decrees	64
	other	58
	foreign materials	39

# INVESTIGATION ACTIVITIES OF THE OFFICE

## ■ 2010 INVESTIGATION PLAN

### I. GENERAL TOPICS FOR SPECIFICATION OF INVESTIGATION ACTIVITIES OF INSPECTORS OF THE OFFICE

#### 1. PUBLIC ADMINISTRATION INFORMATION SYSTEMS

In relation to the previous findings, the investigation activities pursued by the inspectors of the Office in 2010 were again focused on adherence to the duties in personal data processing in the area of public administration. These projects were concerned both with state administration (e.g. the transport information system, information system of a chosen health insurance company, functioning of the pension system and of the state administration in the area of pension security) and particularly with the area of local government (the Office chose one regional authority and one municipal authority for investigation), where problems always occur after recruitment of new officials – personal data protection is overlooked and underestimated, while preference is given, e.g., to the right to access to information; the officials neglect the duty to protect personal data that are part of the files, etc.

#### 2. INFORMATION SYSTEMS IN THE AREA OF PRIVATE LAW

Although private-law systems are not as extensive and interconnected as systems in the area of public law, further development of technologies supporting disclosure of information was also expected in this field, particularly in those areas where a natural person – data subject – acts as a consumer, client, patient, etc. It was therefore found necessary to monitor further development of the legislation and compliance with the approved legal conditions for the operation of large registers and databases, such as personal data processing in relation to the operation of data boxes of natural persons by Czech Post. In relation to the possible investigation into the pension security system, the investigation plan aimed to check personal data processing in the area of insurance. Based on the current knowledge of the method of use of RFID technologies in communication through electronic cards, the persons performing the investigation concentrated on another type of a municipal or student card.

#### 3. INFORMATION SYSTEMS IN THE AREA OF JUSTICE

In respect of the recent development of e-justice information systems, there still persist certain questions and issues concerning the disclosure and exchange of data that are processed in these registers. This is true not only of the area of justice. The Office also focused on other related issues

that pertain to the rights and duties in processing of personal data of all entities involved in this field. While it is undoubtedly true that the legislation provides sufficient legal guarantees preventing any misconduct, it is nevertheless necessary to map out this area, particularly with respect to compliance with the duties pursuant to Article 13 of the Personal Data Protection Act.

#### **4. COMPLIANCE WITH CONDITIONS IN TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES**

Similar to the previous year, in 2010 the Office again dealt with topical issues connected with practical implementation of the conditions for the flow of data outside the territory of the Czech Republic and the EU. Indeed, while "Binding Corporate Rules" are often publicly declared, the Office has yet to check if the responsible entity oversees subsequently compliance with these rules. This intention of the Office is even further complicated by the fact that co-operation will have to be established in this area with another authority or entity that is responsible for the fulfilment of the generally applicable duties in the territory of another country.

#### **5. PROTECTION OF PERSONAL DATA OF DATA SUBJECTS IN CRISIS SITUATIONS**

Based on past experience, the Office found it necessary to continue monitoring the method of processing personal data of persons in difficult life situations or in crises. These people are often under pressure ensuing from their current circumstances and either cannot or are unable to defend themselves against intensive breach of their privacy. Although the adopted legislation has led to substantial changes, particularly to the benefit of privacy of minors, it must still be borne in mind that, in respect of the aforementioned circumstances, the supervisory competence of the Office must also be exercised preventively.

## **II. PLANNED ACTIVITIES AND COMPLETED INVESTIGATIONS FOLLOWING FROM THE 2010 INVESTIGATION PLAN**

### **1. INVESTIGATION AT THE REGIONAL STATE ATTORNEY'S OFFICE IN HRADEC KRÁLOVÉ**

The Investigation at the Regional State Attorney's Office in Hradec Králové was performed within the deadline set in the plan. It was concerned with compliance with all the relevant duties stipulated by the Personal Data Protection Act and Act No. 133/2000 Coll. that fall within the supervisory competence of the Office in respect of processing of personal data of persons involved in criminal proceedings.

No circumstances were found in the Regional State Attorney's Office in Hradec Králové that would cast any doubt about consistent compliance with the parameters stipulated by the Personal Data Protection Act.

### **2. INVESTIGATION AT THE HRADEC KRÁLOVÉ REGION**

The Investigation was performed at the Hradec Králové Region within the deadline stipulated by the plan. It was concerned with processing of personal data in the exercise of state administration in delegated competence and in the exercise of independent competence of a region, i.e. data of the parties to administrative proceedings, persons related to them and other affected persons obtained directly from the data subject through official documents (filled-in forms) or correspondence, as well as similar data obtained from the information system of the records of population or some other list kept for official purposes, and processing of personal data of employees of the Hradec Králové Region and persons entering the premises of the Hradec Králové Region. Again, this investigation aimed at checking compliance with all the relevant duties stipulated by the Personal Data Protection Act and

the Records of Population Act. Seventeen other regulations governing personal data processing, such as the Code of Administrative Procedure, the Archives and Filing Service Act, the Forests Act and the Labour Code, were directly applied in the investigation.

Three measures were imposed to remedy the ascertained shortcomings; administrative proceedings had not been initiated by the end of 2010.

### 3. INVESTIGATION INTO PROCESSING OF PERSONAL DATA OF HOTEL GUESTS

The investigation was concerned with processing of personal data of guests in the context of Article 101 of Act No. 326/1999 Coll., on stay of foreigners in the Czech Republic, which imposes on persons providing accommodation the duty to keep a book of records and to maintain it for a period of 6 years from writing the last entry; and also in conformity with paragraph 1 of the same provision, which stipulates the scope of personal data that are registered in the book of records: the name and surname of the accommodated foreigner; date, month and year of birth; citizenship; passport number; beginning and end of accommodation.

Where a person stays in a spa resort or tourist centre for the purpose of spa treatment or recreation, or where a fee from accommodation capacity is being charged pursuant to Act No. 565/1990 Coll., on local fees, the person providing accommodation is obliged to keep a written book of records, in which (s)he shall record the period of accommodation; purpose of accommodation (the purpose and period are not recorded in the book in respect of a fee from accommodation capacity); name, surname and address of the place of permanent residence or place of permanent residence abroad, and number of the identity card or passport of a natural person to whom the accommodation was provided. Records must be kept in the book of records in a transparent and comprehensible manner. These records must be chronologically arranged. The person providing accommodation shall keep the book of records for a period of 6 years from making the last entry.

Where a spa or recreational resort is not involved, the only available source of information is the contractual relationship. The establishment of a contract is conditional on unambiguous identification of a party – the guest. From amongst the personal data set out in the guest book, unambiguous identification is ensured by the name, surname and number of the identity card.

This method is satisfactory in terms of personal data protection, because while the number of the identity card provides unambiguous identification, such identification is possible only in co-operation with the police.

However, processing of personal data of accompanying persons, i.e. those persons who intend to stay in the hotel, but the rental contract for their room is concluded by someone else, appears to be much more problematic, as the purpose of this processing is unclear. The stated reason, i.e. that the hotel has the right to know who is staying with the guest, does not seem to be a sufficient legal ground for processing of these personal data.

Pursuant to Article 5 (2) of the Personal Data Protection Act, personal data may be processed only with consent or on the basis of a statutory exemption; no such exemption exists in respect of accompanying persons. Processing may therefore be based only on the grounds of consent; however, the latter must be voluntary and cannot thus constitute a precondition for the provision of accommodation. If these data were processed with consent, the period of maintaining these data would be different, as these persons are not those with whom a contract has been concluded, but rather only persons who stayed in the hotel. Data on them should therefore be deleted upon their departure and after the room was checked.

On the basis of the results of the investigation at the hotel, a meeting took place with HORES PLUS s. r. o., which is one of the majority suppliers of software for processing of personal data of guests in hotels; at the meeting, the participants agreed, inter alia, as follows:

The system required only the following data as mandatory: surname, date of arrival and departure, nationality, number of rooms. For other persons, who did not pay for accommodation, the system allowed for keeping records of these persons only by mentioning the number of them and their nationality.

Personal data of guests should be transferred to the Guest Bank only with their consent. Personal data of guests should not be processed or kept in archives for more than 6 years from the last visit.

Logged access by authorised persons was introduced, not only to the archives, but also the Guest Bank, and specially to the item “characteristics”, because this item should be accessed only in case of a complaint by the guest or, in contrast, if (s)he again shows interest in accommodation.

Pursuant to Article 5 (5) of the Personal Data Protection Act, only the name, surname and address may be used in a marketing database; other personal data may be used only with the guest’s consent. Statistics based on characteristics should be drawn up only collectively, i.e. with the use of programmes; there are no legal grounds for making profiles of the individual guests without their consent.

#### **4. INVESTIGATION INTO PERSONAL DATA PROCESSING IN THE INFORMATION SYSTEM OF THE PRAGUE SOCIAL SECURITY ADMINISTRATION**

One of the investigations was concerned with compliance with the duties following from the provisions of Title II of the Personal Data Protection Act by a territorial workplace of the Prague Social Security Administration (TW PSSA) in the processing of personal data of persons insured within sickness insurance.

The purpose and scope of personal data processing are defined by Act No. 187/2006 Coll., on sickness insurance; the methods of personal data processing and the types of operations aimed to achieve the set purpose are stipulated with a binding effect by the Czech Social Security Administration. The individual bodies are authorised to collect data within the scope essential for the performance of their tasks in the area of insurance, including data on the individual insured persons. Insurance information systems include registers of insured persons and registers of employers, which constitute information systems of the public administration pursuant to Act No. 365/2000 Coll. The information systems are not publicly accessible.

On the basis of the findings, it was stated in the investigation record that the TW PSSA had been processing personal data of natural persons (data subjects), i.e. persons insured within sickness insurance, in conformity with Articles 13 to 15 of the Personal Data Protection Act.

### **III. INVESTIGATION AND SUPERVISORY ACTIVITIES IN 2010 – CONDITIONS AND GENERAL CONCLUSIONS**

Two inspectors ceased their activities in 2010 upon expiry of their ten-year term of office. In their stead, the President of the Republic appointed new inspectors, thus renewing the full number of members of the board of inspectors. The continuity of performance of the Office’s investigation and supervisory activities was not thereby impaired.

The principal task within the supervisory activities is to perform state controls and increasing demands are therefore placed on this area, particularly as regards the quality of the individual procedural acts. On the basis of court case-law and of the findings obtained in its own complaint or appellate procedures, the Office modified certain procedures so as to improve the conclusiveness of evidence obtained within the investigation procedure and, at the same time, to strengthen the rights of the controlled entities during the investigation.

The course of the investigations indicates that while, on the one hand, the legal awareness and knowledge of personal data protection is increasing, on the other hand – given the increasing possibilities ensuing from the use of new technologies – there is a constant increase in the number of persons who are totally unaware that they process personal data through modern technologies and thus interfere with privacy of natural persons.

The increasing interest in the protection of personal data is clear particularly in public institutions and major companies, especially in the area of banking, insurance business and large telecommunication

companies. Increasingly often, companies are represented by advisors who specialise in personal data protection.

However, the ratio of not only natural, but also legal persons who avoid investigation or hinder it in any way – particularly by not collecting consignments sent by post or through data boxes and thus avoiding contact with the inspectors – is unfortunately increasing. With growing frequency, the Office encounters a practice where the controlled entities utilise fictitious addresses, at which either no one resides or which do not correspond to reality. In certain cases, the inspectors even experienced that a representative of the controlled company arrived for a hearing without being authorised or empowered to act for the company. These delaying tactics are often motivated by an attempt to achieve expiry of the subjective deadline for the subsequent administrative proceedings. The investigated persons misuse the right to lodge pleas of bias and requests for adjournment of ordered hearings on various grounds. The inspectors have to deal with these facts.

Specific issues are connected with the performance of investigations in the area of the Internet, where the inspectors are limited by competences pursuant to the Electronic Communications Act, according to which the Office is unable to ascertain from the operators of electronic communications traffic and location data of a suspicious entity that hides in the anonymous environment of the Internet or that directly misuses the Internet as a global anonymous tool; the suspicious entity often places illegal information on foreign servers, where it is not possible, not only to find adequate information on the given entity for the above-described reasons, but also to punish the given entity pursuant to the Czech laws.

The only effective instrument available to the inspectors is the option of imposing a procedural fine for failure to provide co-operation, where the upper limit is set at CZK 25,000. This fine may be imposed repeatedly, however, in controls pertaining to electronic communications, only up to the total summary amount of CZK 200 thousand. Furthermore, these proceedings often result in subsequent fast winding-up of companies and founding of new companies by the same persons. However, the year 2010 also confirmed the continuing trend in the approach of complainants, who often do not accept information on the results of investigation findings and question the results of the investigation which state facts other than those which are claimed by the complainants in their instigations. These results in raising complaints about the procedure taken by the inspectors which, in their substance, are complaints against the results of the findings. It should also be stated in this context that there is a constantly increasing number of complainants who misuse the Office for resolving their private-law problems or disputes – in these cases, a suspicion of management of personal data is only a red herring. However, the mere verification of these instigations is time demanding, although very often it must be noted that they are not concerned with the Personal Data Protection Act.

In conclusion of this part, it must be stated that, in spite of budgetary savings, the number of employees involved in supervision was not reduced in 2010; furthermore, it must be noted that, save for exceptional cases, the average duration of investigations was reduced.

# ■ FINDINGS OBTAINED BY INSPECTORS FROM INVESTIGATION ACTIVITIES

## PERSONAL DATA IN HEALTH CARE

The Office found no substantial problems in relation to registration of new personal data controllers in health care. Issues connected with extension of the current registration of large hospitals and health insurance companies have been resolved gradually. These issues include particularly the extension of preventive care, which is organised by health-care institutions in co-operation with commercial entities (e.g. electronic health books, etc.).

The overall number of inquiries, instigations and complaints received was greatly influenced by a case thoroughly discussed in the media: the central depository of electronic prescriptions of the State Institute for Drug Control (hereinafter the "SIDC"), including the subsequent initiative of the SIDC, which aimed to ensure, through a mere change in the SIDC's internal instruction, that information is sent to the central depository of electronic prescriptions. However, such a change may be brought only by law and the Office was therefore again forced to respond to complaints raised by private pharmacies, by the Czech Association of Patients and by individual physicians, pharmacists and patients. Subsequently, there was a rather intensive exchange of views between the Office and the Ministry of Health of the Czech Republic. Based on mutual negotiations, the two parties reached a common conclusion that the relevant legislation, particularly implementing decrees and other sectoral regulations, is not sufficient from the viewpoint of protection of the processed personal data and sensitive data and that it is necessary to introduce a uniform and absolutely clear amendment to the legal regulations.

The Office also recorded a constantly increasing number of complaints raised by patients in respect of incorrect management of their data contained in medical documentation and the related unsecured transfer of information on their state of health among the individual health-care facilities in the provision of health care. The Office reached the conclusion that the area of protection of personal data and sensitive data processed in the sector of health care was being underestimated, not only due to the fragmentation of the legal regulations, but also given inadequate co-operation by the individual bodies and institutions that are involved in the provision of health care.

Save for individual cases of arbitrary conduct of health-care workers, the requirement for consent of the data subject to personal data processing is generally respected and correctly understood in the health-care sector. However, less accepted is the requirement for legality of the purpose of personal data processing, i.e. taking account of whether the purpose of processing of personal data and sensitive data is in conformity with the authorisation of the relevant entities.

It was found that the relevant entities underestimated the requirement for thorough anonymisation of personal data, e.g. in relation to the performance of clinical and non-clinical evaluation of pharmaceuticals and medicinal products, scientific research, as well as accounting to the health insurance companies for trips made by physicians to patients' homes.

In addition to standard complaints about loss or unauthorised management of medical documentation, in 2010 the Office newly encountered lack of confidence of the responsible persons representing health-care facilities in data boxes. In its statements, the Office noted that the responsible ministry was the Ministry of Interior of the Czech Republic and that, from the viewpoint of personal data protection, no facts had been found that would prevent the use of data boxes for communication among health-care facilities, including sending of documents containing sensitive personal data.

The Office provided extensive consultations in relation to personal data processing in the area of personal dosimetry and other systems of radiation protection.

In the course of an investigation performed on the basis of the investigation plan, the Office checked the manner of management of medical documentation in health-care facilities as well as by individual doctors. Although the applicable law (Act on Care for the Health of Population), which stipulates the duties related to management of medical documentation, does not require that physicians and other health-care professionals secure medical documentation against loss, theft or other damage, it refers to the general duty stipulated in the Personal Data Protection Act. Fulfilment of this duty was the subject of numerous controls and non-compliance frequently resulted in penalties. In terms of compliance with personal data protection in management of medical documentation, the Office also checked conformity with the Public Health Insurance Act and the course of registration of patients who choose (or change) their general practitioner. The Office also dealt with instigations concerned with a suspicion of unauthorised management of personal data in relation to the submission of identity cards of deceased patients by hospitals, which requires co-operation with the police, registries of births and deaths and regional health-care departments.

## OPEN CARD

The Personal Data Protection Act was violated in issuing the Prague Resident's Card – the Opencard. In conclusion of the performed investigation, the Office stated that the Capital City of Prague inadequately informed the persons interested in the Opencard on the parameters of future processing of their personal data in a situation where consent of the card user was not required for such processing. The Office simultaneously imposed remedial measures to ensure that every current card holder would be allowed to express his/her consent to or disagreement with processing of his/her personal data, without being limited in the use of the services related to the “Opencard” project, and all persons newly interested in the Prague Citizen's Card – the Opencard – would be enabled to express their free consent to personal data processing already upon submission of their application.

The purpose of the remedial measures is to allow all applicants who do not grant their free consent to processing of their personal data to use the Opencard to the full extent. The Capital City of Prague accepted this conclusion, but simultaneously requested extension of the deadline for compliance with the remedial measures until the end of June 2011.

In addition to the purpose of issuing the Opencard, the Capital City of Prague may process personal data of card holders only with their express consent granted for the reason of easier issue of a replacement card in case of loss or theft.

## STUDENT REGISTERS, PUBLICATION OF DATA OF UNIVERSITY STUDENTS

Personal data of twenty-five persons were published. It follows from the published information that the authors followed from study records kept on the basis of the law. The data demonstrably originated from the student registers maintained by the University of West Bohemia. The University processes these data in an internal automated information system and twice annually transfers them on the basis of the law and implementing guidelines to the Ministry of Education, Youth and Sports, for which the database of data collected from the individual registers is processed by Masaryk University in Brno based on a contract. The Ministry is the manager of the SIMS database and is also directly involved in processing of data from this database. The authorisation stipulated in Article 39 (1) of the Personal Data Protection Act (requirement for collaboration) was also unsuccessfully used to determine the source of escape of the students' personal data. A representative of the MAFRA, a. s. publishing house, the publisher of the Mladá fronta DNES daily, stated with reference to Article 16 of Act No. 46/2000 Coll., on the rights and duties in issuing periodical press and amending some other



laws (the Press Act), as amended, that information on the origin or contents of information published in the periodical /.../ would not be provided.

It was not ascertained during investigations that the students' personal data managed by the controlled entities would escape by fault of specific persons. It was nevertheless ascertained that the controlled entities failed to adequately meet their duties stipulated in Article 13 (1) and (4) (c) of the Personal Data Protection Act.

Fines were imposed in administrative proceedings on all three institutions as entities responsible for personal data processing, within which, as a consequence of inadequate and insufficiently effective security measures, information on law students at the University of West Bohemia were further disclosed and published.

In 2010 the Office also dealt with a series of petitions and provided consultations in respect of an amendment to the University Act, specifically as regards the duty of institutes of higher learning to publish, with effect from 1 January 2006, data listed in Article 47b of the cited Act – dissertations, diploma theses, bachelor's theses and rigorous theses, where defence had taken place, including opponent reports and records on the course and result of the defence, through a database of qualification papers maintained by the school.

Almost simultaneously with the case of non-standard studies at the Faculty of Law, the Office pursued administrative proceedings with the University of West Bohemia in respect of another case of publication of students' personal data. Through a publicly available website, the University published a list of 169 2<sup>nd</sup> year students in the academic year 2009/2010 registered for a state examination and a list of 204 students of the 5<sup>th</sup> year registered in the same academic year for the final summary state examination; these lists contained personal data of the students within the scope of the name, surname, personal number, and date and time of holding the examination. The Office noted that the fact that the course and publication of the results of the state examinations were public did not, in itself, mean that it would be possible to publish on the Internet a list of specific students registered for the individual dates and times of these state examinations. The publicity of state examinations as such does not entail the legal duty in the sense of Article 5 (1) (a) of the Personal Data Protection Act, specifically to publish in advance a list of participants in the examination. A fine was imposed on the University of West Bohemia in Plzeň for violation of the duty stipulated in Article 13 (1) of the Personal Data Protection Act – i.e. the duty to adopt measures preventing unauthorized or accidental access to personal data, their change, destruction or loss, unauthorized transmission and other unauthorized processing, as well as other misuse of personal data.

In connection with processing of personal data of students, Charles University in Prague published data whose publication is not required by the law, without obtaining prior consent of the students to this end. This was a list of 170 students of the 1<sup>st</sup> year in the study field of General Medicine, including the name, surname and date of birth, and assignment of the students to groups for the academic year 2009/2010. The previously determined purpose of processing, specifically maintaining a register of students and provision for organisational aspects of study, was exceeded by publication of the students' personal data. None of the exemptions stipulated in Article 3 (6) of the Personal Data Protection Act applies to the procedure followed by the university.

The University of Economics in Prague published on its website minutes of 18 meetings of the disciplinary committee, which contained personal data of 89 students within the scope of the name, surname, description of the misconduct and type of recommended disciplinary punishment, without having obtained consent of the students to this publication. In this case, the Office also noted breach of the duty to publish personal data only in conformity with the purpose for which they were collected. The Office concluded that meetings of the disciplinary committee are not open to public and considers that the principles expressed in Articles 2 to 8 of the Code of Administrative Procedure must also be applied to the course of the disciplinary proceedings pursued by a public institute of higher learning (university). When determining the penalty, the Office took into account, as an aggravating circumstance, that personal data had been used at variance with the Personal Data

Protection Act in respect of 89 data subjects, and also the fact that the personal data were disclosed through the Internet to a wide range of persons and that information on disciplinary punishment had been published, which can be considered to be a more significant infringement on privacy of the data subjects. Furthermore, the administrative authority took into consideration that the minutes were displayed on the website continuously, for a period of up to six years for the oldest minutes.

In all six cases, which were closed through a final decision, a penalty was imposed close to the lower level of the statutory range and the fines were paid. Of nine remedial measures imposed within two investigations conducted by the Office, six were performed within the deadline stipulated by the inspector; a longer deadline was set for the given controller in respect of the remaining measures that are aimed to provide for the selected technical and organisational conditions.

Publication of data of university students is related to a certain degree to the provision of information on adult students to their parents. In this case, the Office again follows in its decision-making and in answering questions from the University Act, which provides, *inter alia*, in Article 88, for a student register. In this context, a decisive role in terms of making a decision on the right of the parents to obtain information on the course of university studies is played by paragraph 5 of the cited Article, which stipulates that “an institute of higher learning (university) shall provide the relevant data from the student register to a person who has documented his/her legal interest in this respect”. Of course, a legal interest can be associated, e.g. with applying for reduction of the tax base on the grounds of maintenance of students up to the relevant age, usually 26 years. However, in the opinion of the Office, the parent only requires properly documented information that the student has enrolled for the next year of study. Any other details would then have to be considered superfluous in view of the given purpose.

## STUDENT REGISTER

On the basis of a complaint, the Office performed investigation of the Student Register maintained by the Ministry of Education, Youth and Sports and processed by the Institute for Information on Education directed by the Ministry. Information is being rendered anonymous and students are registered under different codes, however so that further information can be added every year, thus yielding temporal series for all students to the extent of 9 to 13 years, documenting the study of each Czech student. This, in fact, results in the creation of a student register, which, in the opinion of the Office, does not fall within the scope of Article 28 of the Schools Act: The Office considers that personal data can be collected, statistically processed and destroyed every year with a view to their processing for statistical purposes. In no case is a purpose defined in this way sufficient for creating a register of all students.

The Student Register also processes data on the *health capacity for education and on health problems that could affect the course of education*. However, pursuant to the law, this information may be processed only anonymously. The method of processing chosen by the Ministry – i.e. that, in one case, every student is characterised by his/her birth number and information on study and, in another case, by a code, information on study and information on health problems – was not anonymous.

## E-MAIL BOX CONTENTS

The Office received a complaint from the former rector of a university who claimed that, following appointment of the new rector, he lost access to the e-mail box that he had had established under his name at the university and, in contrast, the e-mail box was disclosed to the new university management.

Given the fact that the former rector had not used two distinct e-mail boxes, one of which would contain only correspondence with him as the rector of the university, while the other would contain correspondence with him as a teacher or colleague, all correspondence in the e-mail box must be

considered to be his personal correspondence, to which only he should have access, although it uses the university server. The fact that this is a personal e-mail box also follows from the fact that only a given employee has access to his e-mail after logging in with the use of his name and password.

Therefore, once the former rector ceased to hold the office and, in the given case, be an employee of the university, his e-mail box should have been cancelled.

If an e-mail box no longer exists, because the addressee no longer works for the given institution, this information should have been automatically communicated to the sender (who must then take further appropriate steps), potentially with a request for sending the message to the address of the new addressee – in the given case, the new rector. In no case was the university authorised to inspect private mail of its former employee.

## PERSONAL DATA PROCESSING THROUGH CAMERA SURVEILLANCE SYSTEMS

In spite of the fact that today's cameras monitor just about every step we make, the Office has recorded approximately 6 thousand camera surveillance systems in its register of personal data processing, which the Office estimates to be only a negligible part of the systems actually used in the Czech Republic

On the basis of the newly submitted applications for registration of camera surveillance systems, it was ascertained that the share of persons who themselves are not involved in the operation of the camera surveillance systems, but rather outsource this activity to specialised firms, was increasing. The number of these entities has grown by almost 50 % since 2006. It is therefore possible that the collected information could be accumulated by a few specialised companies, particularly security agencies. This was one of the reasons why considerable emphasis was placed in registration procedures on demonstrating compliance with the duties to secure personal data.

Within the submitted notifications of personal data processing, problems were repeatedly encountered in relation to monitoring of employees, customers and clients in waiting rooms, meeting and conference rooms. This trend is apparent in both public and private sectors. The intention to install and operate camera surveillance systems has been declared by schools, hotel companies, restaurants, fitness centres, swimming and bathing resorts, hospitals, municipalities and cities. Although, in the long term, the Office communicates, in its positions and decisions, the conditions under which camera surveillance systems may be operated, new registration notifications continue to suffer from the same issues. These issues include particularly the actual fulfilment of the set purpose, i.e. specifically the placement and setting of the individual cameras and the period of storage of the recordings; indeed, in a number of cases, the period of storage of the recordings considerably exceeded the period generally considered by the Office as appropriate (3 days). Based on request of the Office, the notification was corrected and reduced in scope in almost all these cases.

General statements that sensitive data, particularly biometric data, are being processed through a camera surveillance system continue to be one of the frequent problems that must be resolved within the registration proceedings. Camera surveillance systems using a new technology that can be used to check and identify a specific natural person through certain biometric characteristics (search based on facial elements, walking characteristics, etc.) are the only exception.

A recurring shortcoming in registration consists in the fact that the managers of camera surveillance systems in apartment buildings present their notifications of commencement of personal data processing without the consent of all tenants and replace this by sole consent of the owner or members of the Board of Directors, or only representatives of the individual apartments (e.g. members of the association, members of the co-operative).

Increasingly frequent applications for registration of camera surveillance systems with simultaneous sound recording were a new feature. A vast majority of operators state that the objective of this

monitoring is to protect property, identify offenders, thieves, vandals, etc. Once notified by the Office of inappropriate and disproportionate infringement on the privacy of all the affected persons, a great majority of these operators change the setting of these systems and cease obtaining sound recordings. This is a classical example: availability of technology makes the operators think that “if it exists why not use it”.

A new feature in 2010 can be found in massive attempts to install camera surveillance systems in means of public transit, trains and buses. The Office is very cautious in this respect and consistently assesses each case *ad hoc* with the use of all the statutory means, including particularly initiation of proceedings *ex officio* in the sense of Article 17 of the Personal Data Protection Act in the event that there is a justified concern of violation of the cited Act. The Office does not aim to *a priori* prevent the use of camera surveillance systems to protect the lives and health of the passengers and employees or to protect property, but rather to correct and avoid inappropriate interference with privacy of the passengers.

Co-operation with the relevant institutions in the area of schools and the inspection activities of the Czech Schools Inspectorate has already proven effective in respect to the use of camera surveillance systems, and the methodical work of the Ministry of Education, Youth and Sports contributes to a change in the approach of the individual schools to the use of camera surveillance systems. In fact, no defective practices such as operation of camera surveillance systems in classes, teacher’s offices and headmaster’s offices were found in 2010.

Highly complicated was an investigation performed by the Office’s inspector on the basis of an instigation of the Ombudsman’s representative in two mental hospitals. Given the previous investigation made by the Ombudsman’s office, it was ascertained during an investigation performed by the Office that the operation of the camera surveillance systems had been modified in both hospitals in that they no longer made recordings from the camera surveillance systems and thus did not process the patients’ personal data in the sense of Article 4 (e) of the Personal Data Protection Act. However, the inspector of the Office also noted that, although the mental hospital was used both for health-care patients with normal treatment and for patients placed in the hospital on the basis of a court decision, the aspect of security, including statutory regulation of use of camera surveillance systems, was not dealt with either by the health ministry or by the justice ministry. Representatives of both hospitals almost identically argued that their facilities had experienced attacks against employees, other patients and damage to property. In addition to their health-care work, the facilities thus also substituted for the yet non-existent detention centres, however, without having the powers available to prison facilities.

Mention should be made of a significant increase in the number of applications for consultation from the Police of the Czech Republic, the municipal police forces, municipalities, regional authorities, city halls and other institutions, concerned with the possibility of operating “municipal camera surveillance systems“. Again in co-operation, this time with the Ministry of the Interior, the Office managed to reach a state where these camera surveillance systems employed particularly to prevent street crime are operated by the bodies competent to secure public policy, rather than directly by cities and municipalities.

The number of notifications and cases referred by the Police of the Czech Republic, municipal police forces and individual administrative authorities in cases falling within the competence of the Office also increased in 2010. One of the thus-referred instigations was dealt with in administrative proceedings. It was ascertained and demonstrated that the operator of an accommodation facility installed a camera in one of the rooms and stored the recordings obtained by the camera in his personal computer, while the camera was masked. A fine of CZK 100 thousand was imposed on this operator for this misconduct.

The fact that the approach taken by the Office has been uniform in the long term and thus predictable is witnessed by the fact that the President of the Office dismissed all the remedies lodged in two-instance procedures, including both complaint and appellate proceedings.

## NON-BANKING ENTITIES

Interest among clients in services provided by companies other than banks and similar monetary institutions – i.e. activities of non-banking entities – has been sharply growing recently. Non-banking entities are business companies that are legal entities pursuant to Article 56 (1) of Act No. 513/1991 Coll., the Commercial Code, as amended (hereinafter the "Commercial Code"), founded pursuant to the applicable provisions of the Commercial Code and providing loans to their clients on the basis of executed loan agreements pursuant to Article 497 et seq., rather than banking entities, which are legal entities pursuant to Article 1 (1) of Act No. 21/1992 Coll., on banks, as amended, specifically joint-stock companies also founded pursuant to the Commercial Code, which also provide loans pursuant to Article 1 (1) (b) of the Banks Act, but that, unlike other business companies, require a banking license for the performance of this activity.

These business companies, which do not have a banking license for the provision of products, are called non-banking entities in this chapter. Products provided by non-banking entities seemingly have a number of advantages for clients compared to the usual products provided by banks, and are characteristic for very low requirements on the customer.

However, the apparent readiness of these products leads to light-headed execution of contracts, where the client actually realises the terms of the performance only when using the resulting product. As the client discovers reality, he is increasingly tempted to complain.

These non-banking entities also include companies that offer their clients financial consultancy. In addition to financial advice, these non-banking entities may also offer, through their business agents, financial products of selected banking institutions with which they have concluded relevant agreements.

In the legal relationship to the client whom they acquired and to whom they provide the mentioned advice and consultations or with whom they conclude the relevant contract or contracts, these business agents and partners are in the position of data controller in the sense of Article 4 (j) of the Personal Data Protection Act, because, in these cases, it is them who determines the purpose and means of processing of personal data, performs the processing and is responsible for it. As a result, in this case, these business agents and partners are fully subject to Article 16 (1) of the Personal Data Protection Act, which stipulates that every person who intends as a controller to process personal data or change processing registered pursuant to the Personal Data Protection Act, other than in instances of processing set out in Article 18 of the Personal Data Protection Act, is obliged to notify the Office of this fact in writing prior to commencement of personal data processing.

For identification of their clients, non-banking companies require a great many personal data, which the client provides often before the contractual relationship is concluded.

Complaints concerned with non-banking entities were usually related to the fact that the provided personal data were being misused in connection with the concluded contract.

The most frequent violation of the Personal Data Protection Act ascertained in the controls was personal data processing without consent of the client and redundant collection of personal data. It was ascertained, for example, that data of a customer obtained after conclusion of a loan were also used for some other purpose, or that the controlled company had committed an administrative offence when it processed inaccurate personal data with respect to payments into account, while not complying with the controller's duty to process only accurate personal data; in other cases, personal data were used in a statement published in a newspaper as a response in a dispute concerning a claim of defects of goods.

Deadlines are also often not specified for the storage of personal data; the controlled entities do not sufficiently ensure protection of private and personal lives of the data subjects – they often interfered with the privacy and personal lives of the clients when they made copies of documents containing data providing information on the privacy of persons without any grounds for their processing.

Non-banking entities provide services (usually loans and credit) both directly, where they have the position of a personal data controller pursuant to Article 4 (j) of the Personal Data Protection Act, and also very frequently through other persons. These business agents may then be either independent personal data controllers or personal data processors within the meaning of Article 4 (k) of the Personal Data Protection Act. In this relationship between the controller and the processor, the Office regularly ascertained violation of Article 6 of the Personal Data Protection Act and its controls yielded the general finding that a duly concluded processing agreement is more the exception than the rule.

In numerous cases, the examined entities remedied the ascertained violations already during the investigation. In those cases where this was not so, the Office imposed remedial measures to eliminate the ascertained shortcomings. Based on the results of the investigations, the Office also pursued administrative proceedings against the entities in question; in these proceedings, a penalty was always imposed for violation of the law.

## INVESTIGATION OF AN ASSOCIATION OF APARTMENT OWNERS

In 2010, based on an instigation, the Office performed investigation into compliance with the duties following from the Personal Data Protection Act by an association of apartment owners (hereinafter the “Association”) in the processing of the personal data of apartment owners and their family members, tenants and other persons in connection with issuing electronic chips for the control of access to the apartment building.

In relation to installation of electromagnetic locks, the Association created a database of chips related to the specific apartment owners and, therefore, when passing through the building, the user was thus recorded together with the date and time of arrival or departure.

It was ascertained that, in collecting personal data in connection with the distribution of the chips, some of the owners stated their written disagreement with personal data processing. Consent to personal data processing was not granted by a further seven persons in voting at the meeting of the Association on monitoring of passage through the building.

The Association was imposed the duty to modify the method of processing of personal data of the apartment owners, members of their households, tenants and other persons in respect of issuing electronic chips so that the records of access would not contain personal data of those persons who had not granted their consent to processing of their personal data for the given purpose, or had withdrawn the consent. In view of the purpose of the security equipment, it is sufficient to record entry by an authorised person who was allowed access to the building, without his or her possible identification. The Association also inadequately fulfilled the duty to provide information, as it provided incomplete information on personal data processing in the collection of personal data.

The investigation was therefore completed by imposing the duty to sufficiently provide for consistent fulfilment of the information duty pursuant to Article 11 (2) of the Personal Data Protection Act. A fine was imposed on the company for demonstrated breach of the Act.

## APPLICATION OF THE PERSONAL DATA PROTECTION ACT IN CYNOLGY

There are two cynologic organisations in Europe, and thus also in the Czech Republic, which do not acknowledge the existence of the other.

Dog owners, i.e. also dog breeders, are organised in clubs according to the given dog breeds. Every club follows its own articles and is established pursuant to the Civil Code as a special-interest association of persons.

There is no doubt that a majority of the rules for processing of personal data of dog owners can be incorporated in the articles of the individual clubs and the owners then give consent to processing of their data as the owners of a certain dog by becoming members of the club. However, consent will always be required for other various pieces of information concerning the individual members and/or their dogs if this information is to be posted on the clubs' websites or various written documents.

However, where certain data are further disclosed or published by the owner himself, such processing does not require any special consent, as such consent is already expressed by the owner's conduct. Nevertheless, the scope of thus-disclosed information must naturally be in conformity with its purpose.

## UNSOLICITED COMMERCIAL COMMUNICATIONS

The Office encounters the erroneous belief that Act No. 480/2004 Coll., on certain services of the information society and amending some laws (hereinafter "Act No. 480/2004 Coll.") and the Personal Data Protection Act are not mutually related. The opposite is true: The aspects regulated by the two laws are very closely interconnected in their content.

The Office performs supervision over compliance with the duties stipulated by the Personal Data Protection Act in processing of personal data and is also the competent authority for the performance of supervision over compliance with duties in dissemination of commercial communications pursuant to Act No. 480/2004 Coll.

Where a commercial offer is sent on the basis of non-genuine consent, this constitutes violation both of Act No. 480/2004 Coll., as it involves the actual sending of unsolicited commercial communication, and of the Personal Data Protection Act, because such a personal data controller states erroneous and inaccurate data (i.e. declares that he has available prior demonstrable consent to sending commercial communications). The fact that the two legal rules are not more interconnected in their contents causes real complications in the control process. The Office has pushed for functional interconnection of these laws practically since the actual inception of Act No. 480/2004 Coll.

Some companies argue that, in respect of e-mail addresses that they obtain either from open sources (Internet) or by purchasing a database or other list, they do not state the name and surname and personal data processing is therefore not involved. This argument itself and the fact that they question as to whether or not an e-mail address is personal data, indicates a lack of understanding and knowledge of the definition of personal data, because, in substance, any data may be personal data. All depends on the context. Pursuant to the Personal Data Protection Act, personal data is "*any information concerning a determined or determinable data subject. A data subject is deemed to be determined or determinable if the data subject can be directly or indirectly identified particularly on the basis of a number, code or one or more elements specific to his or her physical, physiological, mental, economic, cultural or social identity*". An e-mail address, as part of the set of information related to a certain person who is the subject of business interest, is undoubtedly personal data.

It may only be questionable as to whether an e-mail address as such is personal data. Here, it is necessary to distinguish addresses that are concerned with a directly determinable entity, such as name.surname@company.xxx, or an indirectly determinable entity. In the former case, this is undoubtedly personal data, while the latter may cause certain doubts. It can be inferred from practice that, if someone creates e.g. the address xxx@gmail.com, he can be identified, even indirectly, only with great difficulties. However, the Personal Data Protection Act does not stipulate for whom a person is identifiable, and it is therefore clear that, for a certain scope of persons, the above-mentioned address is personal data of a person known to them, and it is therefore, in principle, always personal data. It is thus clear that e-mail addresses obtained in the above manner cannot be utilised for sending

commercial communications, because their owner could not have given the relevant consent, either to sending commercial communications or to personal data processing. These cases therefore entail violation of both the Personal Data Protection Act and Act No. 480/2004 Coll.

This aspect also relates to the right of the data subject to access to information on him/herself pursuant to Article 12 of the Personal Data Protection Act. Consequently, if the data subject ascertains or considers that the controller or processor processes his or her personal data at variance with the protection of private and personal life of the data subject or at variance with the Personal Data Protection Act, particularly if his or her personal data are inaccurate in view of the purpose of their processing, pursuant to Article 21 of the Personal Data Protection Act, the data subject may request explanation from the controller or processor and may also claim that the controller or processor remedy the ensuing state of affairs. In these cases, the Personal Data Protection Act provides for blocking, correcting, supplementing or destroying personal data. However, in respect of these requests, it will be up to the data subject to demonstrate to the controller in certain cases that (s)he is indeed the holder of the given e-mail address.

The Office for Personal Data Protection actively commented on amendment to Act No. 480/2004 Coll., which reflects the practice of the Office as a supervisory authority and is also based on experience of similar authorities in the Member States of the European Union. The amendment aims particularly to improve economy and effectiveness of control proceedings and the following proceedings on imposing penalties for the ascertained violations of the Act, and to interconnect the Act with the Personal Data Protection Act as regards procedural provisions, and also reflects the requirements of the European legal rule – new Art. 15a of Directive 2002/58/EC, particularly its paragraph 3.

The Office received 2,834 instigations related to sending unsolicited commercial communication in 2010, of which it resolved 1,525. 163 controls were commenced and 144 controls were completed during the year. 344 complaints were found unjustified (in 288 cases, a commercial communication was not involved and 116 came from abroad); in 120 cases, the sender was not found. A remedial measure was imposed on 578 entities. Administrative proceedings were pursued against 96 entities and fines were imposed on them, through a final decision, in a total amount of CZK 378,000.



## ■ ADDRESSING COMPLAINTS AND PROVISION OF CONSULTATIONS

In 2010, for the first time during the existence of the Office, the public relations department received more than 1,000 complaints about illegal conduct in personal data processing. Over the last 5 years, the number of complaints received during a single year has thus increased almost three-fold, which has required the adoption of corresponding measures, particularly as regards the staff. However, the Office has exhausted all its options in this respect and the only possibility remains to increase the effectiveness of activities in this area of the competence defined by the Personal Data Protection Act, i.e. the initial legal assessment of the contents of petitions in terms of breach of duties in personal data processing, responding to inquiries and applications for legal interpretation, as well as the provision of consultations. On these grounds, the following decision has been adopted for the following year:

Although the Office considers that 10 years from the date of effect of the Personal Data Protection Act has been a sufficiently long period of time for the citizens to adopt a responsible approach to the protection of their personal data and exercising of the rights conferred on them by the legislation vis-à-vis the controllers and processors of personal data, it will control, more consistently than to date, measures of a preventive and awareness-raising nature with the aim to further improve the legal awareness of personal data subjects. Unjustified complaints concerned with violation of the Personal Data Protection Act will be resolved in conformity with the Code of Administrative Procedure through a mere notification that no violation of the law has occurred and the Office therefore found no reasons to initiate proceedings *ex officio*, without explaining this through frequently complicated and time-demanding legal interpretation. Anonymous petitions will be dealt with only in exceptional cases where the Office reaches the conclusion, on the basis of further information, that there exists a public interest in dealing with the given petition. A criterion in decision-making of the Office will lie in the scope of public databases of personal data and the assumption of possible repetition of misconduct by the controllers and processors. Account will also continue to be taken of the complainant's justified concern about being punished by the personal data controller, which concerns are apparent in the long term particularly in the area of labour-law relationships, including a potential risk of losing a job.

## ■ FINDINGS OBTAINED IN ADMINISTRATIVE PROCEEDINGS

After having evaluated the past year from the viewpoint of administrative proceedings pursued and areas where the parties to the proceedings had certain doubts and questions, the Office found that it would be suitable to point out the following problematic issues and provide some comments on:

- the nature of proceedings pursuant to Article 17 of the Personal Data Protection Act;
- the concept of personal data;
- the duty to process only accurate data;
- the provision of personal data in returning credit on anonymous pre-paid phone cards;
- problems related to the Street View service.

### **Nature of proceedings pursuant to Article 17 of the Personal Data Protection Act**

One of the questions on which the Office often commented in the area of fulfilment of the registration duty lies in the nature of proceedings pursuant to Article 17 of the Personal Data Protection Act and the possible form of the Office's decision in these proceedings.

In general, these proceedings are concerned with assessment of whether the Personal Data Protection Act would or would not be violated in the event of personal data processing that has been notified to the Office in conformity with Article 16 of the Personal Data Protection Act. In other words: these proceedings are concerned with the question of whether the controller will breach the conditions stipulated by the mentioned law through the notified processing, which he, as yet, should not or rather may not perform with reference to Article 16 of the Personal Data Protection Act. In these proceedings, the Office follows, on the one hand, from documents gathered in registration proceedings pursuant to Article 16 of the Personal Data Protection Act, i.e. notification of personal data processing and, if appropriate, its supplementation on request of the Office, and specifically its independent registration department, which pursues the registration proceedings pursuant to Article 16 of the Personal Data Protection Act (these proceedings are not administrative proceedings in the regime of the Code of Administrative Procedure – cf. Article 16 (6) of the Personal Data Protection Act), and, on the other hand, from the means of evidence gathered in administrative proceedings pursuant to Article 17 of the Personal Data Protection Act, which are pursued by the department of administrative activities.

While proceedings pursuant to Article 17 of the Personal Data Protection Act are administrative proceedings (in the regime of the Code of Administrative Procedure – and thus subject to application, *inter alia*, of its Article 3), it is nevertheless apparent from the logic of the matter that the proceedings are modified to a certain degree, as the assessment is to be concerned with something that has yet to occur in the future. Consequently, more frequently than in other cases, in these proceedings, the decision of the Office depends on its own discretion and judgment as to whether or not the processing in question, based on the determined or notified parameters of the processing, would result in violation of the Personal Data Protection Act. Proceedings pursuant to Article 17 of the mentioned Act thus play, in actual fact, a preventive role, since these proceedings, or a negative individual administrative act made within the proceedings, may result in prohibition of a certain activity on the grounds of existence of a realistic risk that violation of the Personal Data Protection Act could occur.

In proceedings pursuant to Article 17 of the Personal Data Protection Act, as a rule, the notified processing must be evaluated as a whole, which is then decisive for the potential conclusions of the administrative authority. In this case, the Act assumes that the notified processing will be registered, or that the proceedings will be discontinued on the grounds that the party has given up its intention, or that a negative decision will be issued to the effect that the personal data processing within the scope and with the parameters as notified will not be permitted. It then follows from the above that – although the administrative authority may justifiably consider only a single element of the notified processing to be at variance with the Personal Data Protection Act – this single part will result in the conclusion that the processing will violate the mentioned Act and the notified processing thus cannot be registered, even partly, since the administrative authority is not authorised to make any changes in the notified processing within this type of administrative proceedings unless the party (notifier – potential personal data controller) makes such a change himself. Administrative proceedings pursuant to Article 17 of the Personal Data Protection Act thus involve comprehensive assessment of the notified processing and its conformity with the Personal Data Protection Act.

The following remains to be noted in respect of proceedings pursuant to Article 17 of the Personal Data Protection Act: In proceedings of this type – where it is being determined as to whether the notified processing, as intended by the controller/notifier, will be in conformity with the Act – it is in full competence of the Office (which is authorised pursuant to Article 2 of the Personal Data Protection Act to perform supervision in the area of Personal Data Protection Act) to decide, on the basis of its discretion, as to whether, in the given case, the processing will or will not result in disproportionate interference with privacy of the data subject, particularly in those cases where the notified personal data processing is to rely on grounds recognised by the legal regulations (as set out in Article 5 (2) (e) of the Personal Data Protection Act, with reference to the condition stipulated in the sentence following the semicolon in this provision, in conjunction with Article 10 of the mentioned Act). In the applica-

tion of discretion in these cases, the Office always employs a proportionality test as described, e.g., in rulings of the Constitutional Court of the Czech Republic File No. Pl. ÚS 4/94, Pl. ÚS 15/96, Pl. ÚS 16/98, Pl. ÚS 40/08 and others.

### **A few comments on the term “personal data”**

Beyond any doubt, the basic term, i.e. the concept of personal data, is the most frequently discussed term in the area of personal data protection. In the past year, the Office dealt with several cases in administrative proceedings where the personal data controllers had doubts as to whether the data published by them had the nature of personal data. In this relation, they most frequently argued that the published information has the character of personal data only in relation to those persons, if any, who already know it.

In response to the aforementioned arguments, in the reasoning of its decisions, the Office repeated the following, and currently already traditional and generally acknowledged and generally recognised, approach (or opinion), which is based on the concept of personal data as defined by the applicable regulations of the EU.

Personal data is an absolute term. It is not decisive for how many recipients a certain piece of information constitutes personal data. Personal data is thus any piece of information that can be connected with a specific or determined or determinable natural person. Information that a certain person was at a certain place, that (s)he owns certain property or that his or her movable assets in premises to which (s)he has the right of use are arranged in a certain way, etc., thus also has this nature. Consequently, in terms of Article 4 (a) of the Personal Data Protection Act, personal data means any piece of information that can be attributed to a specific natural person and which thus describes in any way his or her private and personal life, also if the possibility of attributing the information to the given natural person is conditional on a certain necessary knowledge of other facts by its recipient. A fundamental fact, which is dependent on the question of the scope of the necessary prior knowledge of information on a natural person to whom the published data may be related, consists in the degree of infringement on privacy.

### **A few comments on the duty to process only accurate data**

The basic duties of a personal data controller include, pursuant to Article 5 (1) (c) of the Personal Data Protection Act, the duty to process only accurate personal data that the controller obtained in conformity with this Act. Furthermore, this also entails the duty of the controller to update the personal data if required. If a controller ascertains that the personal data processed by him are not accurate, the controller is obliged to take appropriate measures without undue delay, particularly to block the processing and correct or supplement the personal data, or destroy the data. Inaccurate personal data may be processed only within the limits stipulated in Article 3 (6) of the Personal Data Protection Act, where inaccurate personal data must be marked. The controller is obliged to provide the information on blocking, correcting, supplementing or destroying personal data to all (authorised) recipients without undue delay.

However, the category of inaccurate data is not defined only by the fact that the personal data controller processes personal data that do not correspond to the actual state of affairs, but may also be defined by the fact that the controller processes personal data that are incomplete in view of attaining the set purpose – particularly in those cases where the scope of the processed data is delimited by a legal regulation.

To attain any purpose of personal data processing, it is always necessary to have available a certain minimum set of personal data that provide a picture of the identity of a certain person and provide information on other facts (that are related to and decisive for the given case). Where this necessary set of data – particularly if it is determined by a legal regulation and, furthermore, e.g., the ensuing internal act of the controller – is not collected (some data are missing) or where it actually is collected, but the data contained therein are not accurate, it is not possible to attain the set purpose through these

data in the relevant manner. At the same time, such a set of incomplete or inaccurate data gives rise to an incorrect concept of the identity of the data subject, which fact infringes on its personal rights precisely by not corresponding to the reality. Amongst others, for these two reasons, Article 5 (1) (c) of the Personal Data Protection Act requires the personal data controllers to process only accurate personal data and to update these data as appropriate if required.

### **Personal data processing in relation to refund of credit from a pre-paid phone card**

In one of its administrative decisions, the Office dealt with the question of whether a telecommunications operator is authorised to request personal data of persons to whom the operator agreed to refund unused credit in case of cancellation of a pre-paid anonymous telephone card.

In this respect, the Office stated that, for each instance of processing of personal data, the controller needs a legal title, which may consist in consent of the data subject or fulfilment of one of the preconditions stipulated in Article 5 (2) (a) to (g) of the Personal Data Protection Act. In the sense of Article 5 (4) of the Personal Data Protection Act, the data subject must be informed of the purpose of processing and for what personal data the consent is being granted, to which controller and for what period of time. The controller must be capable of demonstrating the consent throughout the entire period of processing. Since the party to the proceedings made the refund of credit conditional on the provision of personal data, it is clear that, in this case, the conduct aimed at the provision of personal data cannot be deemed to be consent that would be a valid legal act within the meaning of Act No. 40/1964 Coll., the Civil Code. The party to the proceedings therefore lacked consent of the complainant, whose personal data it required. It can be added that, in the e-mail message by which the complainant provided his personal data to the party to the proceedings, the former simultaneously stated that he did not provide consent to their processing. Moreover, in respect of the statement of the party to the proceedings, it can be concluded that the provisions of general terms and conditions cannot replace and do not constitute consent of the data subject to processing of his personal data within the meaning of Article 4 (n) of the Personal Data Protection Act.

The Office thus dealt with the question of whether personal data may be processed for the set purpose without consent of the data subject, i.e. on the basis of one of the exemptions set out in Article 5 (2) (a) to (g) of the Personal Data Protection Act. In the case of the party to the proceedings, it is possible to consider potential application of Article 5 (2) (b) and (e) of the Personal Data Protection Act.

Pursuant to Article 5 (2) (b) of the Personal Data Protection Act, it is possible to process personal data without consent of the data subject provided that such processing is necessary for the performance of a contract to which the data subject is a party or in case of negotiations on concluding or amending an agreement that take place on the basis of a proposal by the data subject. In this case, the Office had to conclude that, if the service was activated for the complainant and was used without the party to the proceedings needing his personal data, the party was not authorised to require these personal data upon its termination and refund of the remaining credit. Therefore, where personal data are not required for concluding a contract, the Office considers that they will also not be required for its termination.

Processing of personal data without consent of the data subject where required for the protection of the rights and legally protected interests of the controller, recipient or some other affected person is permitted by Article 5 (2) (e) of the Personal Data Protection Act. For the purposes of identifying the person to whom the remaining credit is to be paid (which was the main reason why the party to the proceedings requested personal data from the complainant), it undoubtedly suffices to require that the given person submit the original SIM card together with the accompanying letter containing PIN and PUK codes, together with the number of the bank account to which the balance is to be transferred. Personal data are therefore redundant and requesting these data is at variance with the principle of the activated service, which is anonymous; the SIM card is transferable and, therefore, the final card holder may differ from the one who activated it. From this also follows the card holder's entitlement

to claim a refund of the credit, without regard to his identification. Moreover, the Office noted that sending a copy of an identity card by e-mail is not a relevant means of evidence in the event of fraud and the party to the proceedings can in no way be certain that this is actually the identity card of the applicant. Also for this reason, a request for the provision of a copy of an identity card and personal data stated therein cannot be considered necessary for identification of the applicant for a refund of the remaining credit.

### Street View

On 18 February 2010 a company having its registered office in the territory of the Czech Republic notified the Office, pursuant to Article 16 (1) of the Personal Data Protection Act, by means of a registration form, that it intended to operate the Google Street View service, i.e. that it intended to process personal data for the purposes of providing this service. In its notification, the company stated that, in the provision of the Google Street View service, photographs would be made of streets and other places that have the status of public premises in the sense of the legal regulations. The photographs would be taken during normal every-day traffic and the photographs would depict all the persons and vehicles present at the specific time of passage of a special vehicle taking the photographs at the given place, as well as all the buildings and land located in the vicinity of the road along which the vehicle would be driven.

In the given case, the Office found that personal data would be gathered during taking of these photographs. In this conclusion, the Office followed from the fact that the quality in which the photographs were to be taken would be sufficient for identifying the persons depicted on them. In this relation, the notifier stated that the faces of the persons would be blurred. In this respect, the Office noted that this fact was relevant only partly, both because, according to the notifier, the faces would be blurred only after the imagery would have been transferred to the U.S.A. and because, in spite of partial blurring of the face, the person depicted on the published photograph would be identifiable by certain data recipients.

In respect of the scope of the processed personal data, the Office also reached the conclusion that, in addition to the personal data pertaining to the given person, i.e. particular data indicating that the person was present at a specific place, etc., the pictures taken would also contain further personal data. Specifically, they would depict houses, properties, cars, arrangement of things on a property, etc. In this relation, the Office noted that, in the sense of Article 4 (a) of the Personal Data Protection Act, personal data means any information that provides a description of a natural person or his/her private and personal life and can be connected with the given data subject by at least a certain group of recipients.

The given personal data processing was to rely on a legal ground acknowledged by law and stipulated in Article 5 (2) (e) of the Personal Data Protection Act.

In general, when determining whether an exception allowing personal data processing without consent of the data subject can be applied within the given provision, it is necessary to evaluate (in terms of priority), in view of the condition stipulated in the sentence following the semicolon in this provision, which stipulates that personal data processing “*may not be at variance with the right of the data subject to protection of his/her private and personal life*”, based on the proportionality test, the relationship between the right of the data subject to privacy and the interest that is to be achieved (protected) by processing personal data. The mentioned test was employed, e.g., by the Constitutional Court of the Czech Republic in its Award File No. Pl. ÚS 4/94, or, e.g., the European Court of Justice in Fedesa (C-31/88, (1990) ECR-4023).

After having taken the proportionality test (in simple terms), the Office reached the conclusion that, taking into consideration, in addition to the above, particularly the declared height (2.7 m) of the camera that was to take the pictures, i.e. in respect of the fact that the pictures taken would provide a view from a greater height than normally possible (moreover, the notifier also intended to take pictures from areas closed to trucks, from which such a view would be potentially possible, and

also from areas closed even to passenger cars), implementation of the notified project of personal data processing would constitute a disproportionate interference with the rights of the data subjects to protection of their private and personal lives, i.e. the right to protection of privacy (protection of personal data) in this case overrode the interest pursued by the processing of personal data.

In other words, the Office came to the conclusion that the conditions for processing personal data on the basis of the legal title set out in Article 5 (2) (e) of the Personal Data Protection Act would not be fulfilled, i.e. the notified personal data processing would be based on no relevant legal grounds (basis in law).

Therefore, in this case, based on the contents of the notification of personal data processing and its supplementation based on request of the Office, there was a justified concern in the sense of Article 17 (1) of the Personal Data Protection Act that the processing of personal data in the form as notified could result in violation of the law. On the basis of this concern, the Office then initiated administrative proceedings *ex officio* pursuant to Article 17 of the mentioned Act and, in these proceedings, having performed the relevant procedural steps with reference to the above-mentioned facts and having ascertained the facts of the case within the scope of Article 3 of Act No. 500/2004 Coll. (subject to the limits described above in the section “Nature of proceedings pursuant to Article 17 of the Personal Data Protection Act”), it ruled that the notified processing did not fulfil the conditions stipulated by the Personal Data Protection Act, particularly because its implementation would result in breach of Article 3 (5) (b), Article 5 (2) and Article 10 of the aforementioned Act. For this reason, the Office then rejected the notified processing of personal data.

The notifier then lodged an appeal against the decision of the 1st instance administrative authority with the President of the Office. The President of the Office subsequently upheld the decision of the first instance administrative authority.

## REGISTRATION

Similar to previous years, the trend of an increasing number of registration notifications continued in 2010. During 2010, the Office received 4,037 notifications of processing data pursuant to Article 16 of the Personal Data Protection Act. This marks a 23.2% increase compared to the previous year. In addition to assessment of registration notifications received, the Office issues decisions on cancelling registration pursuant to Article 17a (2) of the Personal Data Protection Act. A total of 119 instances of processing were thus cancelled during 2010 on 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. Here, in contrast, the number decreased by 14.4 %. The Office publishes information on cancelled registrations in its Journal. In connection with the increasing number of registration notifications, there have also been an increasing number of notified changes and supplements to previously registered instances of processing. The changes are most frequently concerned with addresses, supplementation of the scope of the processed personal data, categories of data subjects and supplementation of the purposes of processing.

## TRANSFER OF PERSONAL DATA ABROAD

In 2010 the Office recorded a decreasing number of applications for authorisation to transfer personal data to third countries. This trend was caused particularly by the fact that the controllers increasingly used, for the transfer of personal data to third countries, instruments created by the European Commission specially to secure adequate protection of the transferred personal data in the third country and which thus allow the controllers to transfer personal data in the regime of Article 27 (2) of the Personal Data Protection Act, i.e. without special authorisation by the Office.

These instruments include particularly “Safe Harbor”, which is a tool regulated by the Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and which was specifically established for the transfer of personal data to the United States of America. The Office recommends to the controllers (exporters of data) to check, before the actual transfer, whether the certification of the relevant organisation is still valid, whether and in what manner natural persons are informed of the internal procedures for dealing with complaints, and whether the “privacy policy” of the given company in the United States is publicly accessible, e.g. through a website. If any shortcomings are found in the application of the principles of “Safe Harbor”, it is appropriate to inform the Office.

This year, the Office also recorded 50 cases where data were transferred pursuant to the Commission Decision on standard contractual clauses. A fundamental change in the area of application of contractual clauses was brought about by Commission Decision 2010/87/EU of 5 February 2010.

Based on the exemption set out in Article 27 (3) (b) of the Personal Data Protection Act, the Office may permit a transfer to a third country if the controller provides for sufficient protective measures for the protection of privacy and fundamental rights and freedoms of persons. Protective measures may follow particularly from Binding Corporate Rules (BCR).

With respect to the fact that multinational companies usually do not have their headquarters in the territory of the Czech Republic, the Office has yet to be requested to become the lead authority that would co-ordinate the entire authorisation process within the EU.

As regards the actual applications for authorisation to transfer personal data to third countries, controllers most often rely on Article 27 (3) (a) of the Personal Data Protection Act, i.e. transfer of data with consent or on the basis of an instruction of the data subject. The authorisation was concerned

mostly with transfer of employee data (basic contact details, as well as data on the position of the employee within the structure of the international group, and exceptionally also other data, such as the amount of salary and awarded bonuses) within a multinational corporation for the following purposes: ensuring participation of employees in educational programmes, establishing an internal social network, accounting for travel allowances, engagement of employees in the employee stock programmes, management of remuneration and bonuses within the group.

In case of a transfer based on consent, this is in fact a derogation from the principle of adequate level of protection in the country of destination, as expressed in Directive 95/46/EC and thus also in the Personal Data Protection Act. This derogation allows for transfer of data to third countries that do not ensure an adequate level of protection. For an individual, this means that his personal data will not be afforded the same protection in the country of destination as that guaranteed by law in the Czech Republic. In these cases, the Office therefore especially strived to ensure that, in conformity with Article 5 (1) (d) of the Personal Data Protection Act, only personal data required to attain the set purpose were transferred and that the consent of the data subject to the transfer of his personal data to a third country complied with the requisites of Article 4 (n), Article 5 (4) and Article 11 of the Personal Data Protection Act, i.e. that the consent was a free, conscious and informed manifestation of will of the data subject, which could be demonstrated by the controller throughout the term of the processing. Apart from consent, in most cases, an authorisation for the transfer was issued on the basis of compliance with the requirement of Article 27 (3) (e) and (f), according to which a transfer is possible if this is required for the performance of the contract to which the data subject is a party or if this is necessary for the performance of a contract concluded in the interest of a data subject between the controller and a third party. This was the case particularly in respect of travel agencies that transfer personal data of their clients to hotels and other business partners who arrange the stay of the clients of the given travel agency in a third country.

### **PNR data**

In 2010, the European Parliament postponed voting on its consent to final conclusion of the preliminarily functioning bilateral treaties on processing and transfer of the Passenger Name Records (“PNR data”), which had been negotiated by the European Union with the United States of America and Australia.

The European Commission therefore announced its plan to define, prior to commencement of bilateral negotiations on the aforementioned treaties, a uniform standard of transferring PNR data, specifically within the Communication from the Commission of 21 September 2010 on the global approach to transfers of Passenger Name Record (PNR) data to third countries. European personal data commissioners reacted to this material in the statement of the European Data Protection Supervisor and also in statement 7/2010 (WP 178) of the WP 29 working group for data protection.

With reference to the basic principle of data protection, i.e. the principle according to which it is possible to collect and process only data required to fulfil the set purpose, both the above-mentioned statements also point out the pressing fact that there has yet to be drawn up an analysis to prove that mass transfers of personal data on passengers from the reservation systems in any way contributes to fighting terrorism and serious international crime.



# LEGISLATIVE ACTIVITIES

2010 was a year of active preparation of several legal regulations that are inherently related to protection of privacy.

One of the most important tasks in which the Office was involved was the work of an expert group concerned with developing a **legal regulation on processing samples of human DNA**. International comparison of legal regulations concerned with DNA showed that the Czech Republic was one of few European countries lacking robust legislation concerning police DNA databases, where processing of DNA by the police can currently be regulated to a considerable degree by a mere order of the Police President. It can be anticipated that the results of the work of the aforementioned expert group will form a future basis for the preparation of one or more legal regulations concerned with treatment of human DNA.

In respect of an issue that was frequently publicly discussed, namely **camera surveillance systems**, the Office commented on a draft legal regulation in this area. The draft was not finalised in 2010. The Office considered it more suitable to proceed solely with legal regulation of the frequently problematic and discussed cases of cameras used on public premises or other publicly accessible places. In respect of certain other specific surveillance systems and technologies allowing for surveillance, the Office stated that, in its opinion, it would be suitable to stipulate more detailed rules and procedures in special regulations, also covering personal data processing.

In the area of justice, the Office welcomed the fact that the Ministry of Justice had finally reconsidered the purposefulness of **personal data processing within the database and on-line portal of the Commercial Register**. However, the Office still does not consider the achieved state of affairs satisfactory, because it is necessary that registers and records in the area of justice be dealt with comprehensively, taking into consideration the possibilities and dangers associated with electronic data processing on the Internet and also given the new services of e-Government.

In relation to an amendment to the **Criminal Records Act**, the Office pointed out that a great many extracts are commonly requested in both public and private sectors from this register of very sensitive data. The Office therefore recommended to deal, in addition to preventing the falsification of extracts, also with alternative options of securing all forms of extracts and increased risks of misuse in electronic applications for extracts made by public authorities.

In 2010, the Office continued to record a continuing interest in creating a legal regulation in the area of **monitoring the consumption of pharmaceuticals and management of prescriptions through a centralised database**. The Office supported an unambiguously defined method of

recordkeeping and supervision of management of pharmaceuticals that are commonly abused (including all persons who come into contact with these pharmaceuticals). However, its proposal was not employed by the Ministry of Health. Nevertheless, it unequivocally refused the possibility of extending the contemplated measures to all patients using medicaments that are not abused. The Office considers it fundamental that a detailed discussion in society as well as in professional circles take place and that all the impacts and risks be evaluated prior to making a proposal for a central database of sensitive data, i.e. also including the proposed register of medical records of patients, which has not yet been the case here.

From the viewpoint of the competence of the Office and its activities particularly in the area of electronic communications and services of the information society, of fundamental importance in 2010 was the commencement of **implementation of Directive 2009/136/EC**. The Office submitted a number of comments on the Electronic Communications Act (over which it also performs supervision in the area of personal data protection). The Act specifies the rules of personal data protection (e.g. provisions concerning access to personal data of the users) and further details of the competence in supervision over personal data processing. Given the fact that discussion of administrative offences consisting in violation of the rules of personal data processing in electronic communications logically follows on from the procedures of the Office pursuant to the Personal Data Protection Act, the Office proposed to reconsider certain penalty provisions of the Electronic Communications Act, which duplicate provisions of the Personal Data Protection Act, and to incorporate penalties for special offences in the Personal Data Protection Act.

The Office also performs supervision over provisions of the Act on Certain Services of the Information Society and it therefore welcomed the fact that the aforementioned Directive requires **availability of information necessary for investigating unsolicited commercial communications**. It is fundamental in terms of law enforcement in the area of the Internet that it be possible to verify the identity of the persons who operate electronic means that are used to disseminate the annoying unsolicited messages. It is therefore desirable from the viewpoint of the Office's capacity as a supervisory institution that the law clearly require collaboration of these persons in official proceedings, that it stipulate the relevant forms of provision of collaboration to the Office and that it be simultaneously clear what information can be requested in proceedings held by the Office. Furthermore, on the basis of its experience obtained in investigations performed to date, within commenting on the amendment, the Office suggested that emphasis be placed in the area of commercial communications on really serious cases and that criminal punishment be imposed only in cases of extensive and repeated sending of unsolicited commercial communications.

In respect of the new Civil Code, the Office has recommended in the past that a more up-to-date and practical regulation be adopted – particularly in view of the possibilities ensuing from modern technologies – for the **acquisition of video and sound recordings of persons**. Instead of clearly stipulating the legal conditions from which it would be possible to infer the need for or at least the limits of making such recordings, the authors of the Code merely stated that the affected persons entering the monitored premises agreed with such surveillance. The Office considers this approach to the protection of privacy of citizens to be short-sighted and at variance with the fundamental principles of personal data protection. In the upcoming commentary procedure, it will therefore require that the relevant provisions be clarified.

In conclusion of the year 2010, the Office received a request for its opinion on the draft **Government Strategy of Combating Corruption** for the period from 2010 to 2012. The material submitted to the Office contained a number of legislative measures directly concerning the issue of personal data protection (e.g. a change in the conditions of tapping telecommunications and use of a police agent pursuant to the Code of Civil Procedure, development of data sharing and protection within the Police of the Czech Republic, analysis of whistleblowing and protection of persons reporting corrupt practices).

The Office noted that specific measures must respect the principles of personal data protection and thus need to be formulated in practice so that they allow for processing and disclosing personal data only for exactly specified purposes and that they are available only to clearly delimited authorised bodies, under exactly specified procedures and to an extent absolutely necessary for fighting corrupt practices.

In respect of the introduction of a **register of misdemeanours**, the Office pointed out that it was not entirely clear why it was necessary to fully centralise the records of misdemeanours in various areas of human life, and noted that the regime of the register of sensitive data had to contain adequate explicit guarantees (legal rules) for processing of personal data, similar to the strict model of the criminal records. As regards the introduction of “**reliability tests**” for other persons working in public authorities, the Office objected that this new institute would be concerned with officials who are not in a service relationship and their labour-law relationship is governed by the general legislation. In case of this major group of persons, provocation appears to be an excessive interference with their privacy. With respect to an electronic register of protected information obtained from financial institutions (**central register of accounts**), the Office questioned the proposed centralisation of data, since the currently applicable legal regulation provides a number of competences and, at the same time, also mechanisms preventing misuse of data. The objective pursued by the register affects practically all the citizens of the Czech Republic; in view of the presented statistics of detecting corruption in the previous years, this constitutes extensive monitoring, which is a very questionable intention. The Office requested that all the above-described topics be paid attention as early as in the phase of preparatory work and demanded that it be consulted already in the phase of preparation of substantive intentions of legislative changes.

# RELATIONS TO FOREIGN COUNTRIES AND INTERNATIONAL COOPERATION

In 2010 the Office had the honour to host a prestigious **European Data Protection and Privacy Commissioners' conference** held on 29 and 30 April in Prague. The event was attended by over one hundred delegates from a majority of European countries; papers were presented not only by representatives of the European data protection authorities, but also by representatives of the European Commission, Council of Europe and scientists, also from overseas. The motto of the conference "**Weighing up the Past, Thinking of the Future**" was echoed in the entire programme of the conference and not only reflected, e.g. the importance of new, particularly technological trends of personal data protection, but also described the beginning of 2010 as a time of considerations before the preparation of revision of the basic European regulation in the area of personal data protection – Directive 95/46/EC.

The Conference was divided to the following thematic sessions: "**Internet of things; ubiquitous monitoring in space and time**" was concerned with the technological phenomenon affecting practically every individual in modern society and showed how technology influences the current concept of privacy. The topic of another session, "**Children in cweb on networks**", was closely related to the previous topic and focused on young people, who often perceive the opportunities and pitfalls of the world of modern technologies in a different way than the older generation. The session "**Personal data protection at the crossroads**" was dedicated to considerations and ideas related to modernisation of the European personal data protection law. The topic of the fourth session is clear from its title: "**Public sector: respected partner or privileged processor?**" – it was concerned with specificities of personal data protection in an area where authorisation to process citizens' data is traditionally conceived as a matter-of-fact competence of the state and its authorities – however, it is becoming increasingly apparent that public authorities do not always provide adequate guarantees of appropriate processing and security of personal data. The final specialised session of the conference was dedicated to the aspects of **ethnic profiling**.

The **conference resolution**, which was discussed directly at the conference and subsequently adopted and which deals with aspects of further development in the area of (legal) protection of personal data and privacy, preparation of joint steps concerned with awareness and education of young people at European and international level, the need for and conditions of use of body scanners for security purposes at airports, and the aspects of the mechanism (agreement) being prepared with respect to standards of personal data protection between the U.S.A. and EU in the area of police and judicial co-operation, can be considered a summary of the work of the conference.

The European conference showed a viable potential of the principles of data protection in globalised society, while using new technologies and data processing on the Internet. In view of these trends,

the year 2010 was dedicated, within foreign agenda of the Office, to revision of the rules of personal data protection and discussion of entirely new rules.

Primarily, the planned revision of the central and traditional European legislative document, the Directive 95/46/EC, was dealt with by the **Article 29 Data Protection Working Party** (WP 29), of which the Office is permanent party, both at their plenary meetings and subgroups, in which representatives of the Office were regularly involved.

Active membership in this group, emphasised by the fact that **the President of the Office, Dr Igor Němec, was elected Vice-Chairman of WP 29** in 2010, allows the Office to present own findings and experience at supranational level and thus contribute to the creation of pan-European approaches to regulation of personal data protection.

In addition to WP29, as in previous year, the Office was engaged in 2010 in the work of other **European formations, particularly the joint supervisory authorities**. A representative of the Office, Dr Miroslava Matoušová, participated in the inspection of joint control authorities in Europol and Eurojust and also worked as an expert on the regular evaluation of the level of personal data protection in implementation of the requirements of the “Schengen acquis” (i.e. the Schengen Convention and related legal documents) in Spain and Portugal.

The same attention was paid to a change in the approaches to personal data protection elaborated by the advisory panel of the **Council of Europe** for Convention No. 108 on automated processing of personal data. In June 2010, Dr Hana Štěpánková was elected its first Vice-Chairwoman.

In the past years, the Office also gained experience and professional recognition in the EU-funded twinning projects. This was one of the reasons, why the Office, and directly its employees, was asked in 2010 to **join the international teams** concerned with evaluation of the standards of personal data protection and the position of the competent data protection authorities in countries introducing or improving their personal data protection. Employee of the Office Dr Jiří Maštálka became the **key expert in a project in Albania**, focusing on revision of the legal framework for personal data protection and optimization of the procedures of the Albanian authority entrusted with supervision over data protection. The Office nominated **4 short-term experts** for a similar project in Macedonia scheduled for 2011.

At the request of the **Bulgarian Personal Data Protection Commission**, the Office organised a **two-day workshop** in Prague in autumn of 2010, where it acquainted its Bulgarian colleagues with practical **findings obtained** in the Office’s **supervisory procedures**, particularly with respect to Schengen issues.

Two working meetings of experts from the Polish, Czech and Hungarian authorities working **on a joint international project funded under the European Union’s Leonardo da Vinci programme** were organized by the Office in 2010 in Prague. The persons responsible for this project aim to raise awareness of personal data protection among the professional and lay public in business circles and in labour-law relationships. The project should yield a guideline that will offer the employers and employees comprehensible and useful information on the conditions of processing and protection of data and provide instructions as to how should the given persons proceed in various situations in business.

Especially intensive work was necessary at the European level in 2010 in respect of treaties between the U.S.A. and the EU on personal data protection in police and judicial co-operation, i.e. an issue that has already been discussed for several years. In this respect, the Office repeatedly raised, with more or less success, comments on the draft national position of the Czech Republic on the entire issue; however, it can be anticipated that a more fundamental role will be played by an expert call addressed by the national data protection authorities at the end of the year to the European Commission from the position of the aforementioned working group, WP29, and which contains a summary of problems apparent in the current draft general agreement between the U.S.A. and the E.U. (the umbrella agreement).

A milestone in the area of transfers of passengers' data in air transport to third countries (the PNR agenda) was laid in 2010 by the Communication from the Commission of 21 September 2010 on the global approach to transfers of Passenger Name Record (PNR) data to third countries. This document takes into account comments of personal data protection authorities, a number of which were also provided by the Office in the past years.



Participants of European Privacy and Data Protection Commissioners' conference  
Photo: Pavel Hořejší

# THE OFFICE, MEDIA AND MEANS OF COMMUNICATION

In 2010, the Office focused its communication with the media on active daily service and provision of up-to-date information through its website.

At the winter press conference traditionally organised on the occasion of the Data Protection Day, the Office launched the fourth edition of the competition for children and youth called “My privacy! Don't look, don't poke about!“, which aimed, this year, to bring attention of children and young people to the risks connected with communicating through the Internet and utilising social networks.

The interest among journalists in press conferences organised by the Office is stable – the conferences are attended by 20-25 journalists. However, it may be deemed important that a whole range of the media scene is represented – agencies, electronic and print media. The number of reports published in the media in respect of personal data protection as a follow-up to the press conference, was similar in 2010 as in the previous year (30 to 60 outputs in 3 days after the press conference). In annexes to press releases, the Office regularly provides information on investigations closed by initiation of administrative proceedings. The Office considers that, with a view to disseminate knowledge of personal data protection in the media and, in turn, among the general public, it is suitable to publish the reasons for imposing fines, where it perceives a possibility of organically improving legal awareness of the methods of application of the Personal Data Protection Act.

## Website of the Office

In the last month of 2010, the Office opened on-line discussion forum in respect of the topic of use of customer (loyalty) cards. By answering a number of questions, it pointed out, *inter alia*, the risks connected with the provision of personal data, on which the provision of a customer card is conditional. The Office resolved to use the option of a discussion forum to find out to what extent the public is aware that the need for protection of privacy is also connected with the use of client or loyalty cards. It appears that the reactions, which are permanently available on the website in the Discussion Forum / Closed Forums / Customer Cards, are mostly based on defence of this marketing strategy; unfortunately, it is clear that the citizens are either absolutely uninterested in the possible consequences of monitoring private life or are not interested because they are not sufficiently informed of utilisation of their personal data, or they prefer even a marginal financial benefit to protection of their own privacy, or the opinions presented in the discussion originated from professional marketing professionals, rather than from citizens. In any case, it proves to be justified that the Office performs its supervisory competence in this area.

### Library and publications of the Office

The library continues to serve as a professional basis for employees of the Office, but is also open on individual request to professional public. It is used by students for their seminary papers and diploma theses concerning personal data protection.

In 3 volumes of its Journal, the Office published important foreign documents on protection of personal data, as well as fundamental statements of the Office. The published documents are also available in electronic form and can be found on the basis of published contents of the individual volumes of the Journal.

The information bulletin, which has been issued since 2010 exclusively on selected topics, was dedicated to the aspects of protection of privacy of children communicating on the Internet. Under preparation is an issue focusing on the aspects of DNA – in relation to protection of privacy and issues of the desirable legislation on use of DNA.

In 2010 the Office intensified **co-operation with institutions**. This includes particularly the newly commenced co-operation with the Union of Cities and Towns, improved co-operation with the Czech Telecommunication Authority and with the U.S. Chamber of Commerce.





# ORG INFORMATION SYSTEM

Act No. 111/2009 Coll., on basic registers, and its amendment through Act No. 100/2010 Coll., imposed a new task on the Office: By 30 June 2012, to create the ORG Information System as part of the system of Basic Registers, which shall provide for processes connected with identification of natural persons.

Financing of the investment part of the required system was ensured through Resolution of the Government No. 1019/2009 and the project is co-financed by a European Union project to the extent of 85 % of the eligible costs, based on a legal act on the provision of subsidy of 30 November 2010.

The basic aim of the ORG Information System (which is described, in certain materials, as an identifier converter) is to provide for protection of personal data within the entire system of the Basic Registers by means of replacing the current use of the birth identification number as a universal identifier of natural persons by a system of meaningless identifiers. These identifiers will differ for the individual agendas or groups of agendas and will thus not allow for search for information on a natural person in a different agenda based on knowledge of one identifier. The only place where all these identifiers will be stored is the ORG Information System. However, this system will not contain any names of natural persons and, therefore, even knowledge of all the identifiers will not enable the Office to determine how they are assigned to the individual natural persons. In this way, implementation of the project of Basic Registers should substantially contribute to the protection of personal data of citizens.

The ORG Information System is implemented in the system of Basic Registers within the Integrated Operational Programme, the priority axis Modernisation of Public Administration.

The public contract for the design and supply of the ORG Information System was commenced on 27 November 2009. On the basis of announcement of this contract, the Office received a total of 6 bids. The tender for supply of the ORG IS was won by TESCO SW, a.s.

Adoption of Act No. 100/2010 Coll., amending Act No. 111/2009 Coll., on basic registers, extended the period of the pilot operation of the system, where the commencement of normal operation is envisaged in the Act as of 1 July 2012.



# STAFF

The Office was allocated 102 functional positions by the 2010 state budget. On the basis of Government Resolution No. 715/2009, the number of functional positions was decreased by 5 compared to 2009 and subsequently increased by 12 on the grounds of competences assigned to the Office under Act No. 111/2009 Coll., on the basic registers. As of 1 January 2010, the Office had 93 employees. 51.0 % of the Office's employees are women, 61.5 % of employees have university education.

# ECONOMIC MANAGEMENT OF THE OFFICE

The Office's budget was approved by Act No. 487/2009 Coll., on the state budget of the Czech Republic for 2010.

## WITHDRAWAL OF CHAPTER 343 OF THE STATE BUDGET – OFFICE FOR PERSONAL DATA PROTECTION

in CZK thousand

### Summary indicators

Total income	6 665.78
Total expenditures	96 732.95

### Specific indicators – income

Total non-tax and capital income and accepted transfers	6 665.78
of which: total income from the budget of the European Union	41.05
other non-tax and capital income and accepted transfers. in total	6 624.73

### Specific indicators – expenditures

Expenditures to ensure performance of the tasks of the Office for Personal Data Protection	96 732.95
--	-----------

### Cross-cutting expenditure indicators

Salaries of employees and other payments for performed work	48 883.00
Mandatory insurance premiums paid by the employer *)	16 620.00
Contribution to the Cultural and Social Needs Fund	935.00
Salaries of employees within an employment relationship	38 099.00
Salaries of employees derived from salaries of constitutional officials	8 613.00
Total expenditures co-financed from the budget of the European Union	249.76
of which: from the state budget	31.31
contribution from the EU budget	218.45
Total expenditures recorded in the information system of programme financing	4 890.50

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

# PROVISION OF INFORMATION PURSUANT TO ACT NO. 106/1999 COLL., ON FREE ACCESS TO INFORMATION, AS AMENDED

In 2010 the Office received twenty requests for information pursuant to the Free Access to Information Act.

Two requests were rejected and, in two cases, the Office issued a decision on partial refusal. In none of these cases, the decision of the Office was challenged by the applicants – through an appeal to the President of the Office. The procedure of the Office in dealing with requests for information was not contested by any complaints pursuant to Article 16a of the Act on Free Access to Information.

Most often, the applicants requested that they be provided with specific administrative acts or other official documents of the Office, and also with information on proceedings initiated based on their instigation; they also requested other documents of the Office, such as its internal regulations, the 2010 control plan, etc. The Office was also requested to disclose information on the number of small contracts and the amount of these contracts which it granted in 2007, 2008 and 2009, as well as information as to whom, for what services and what amounts it paid in 2009 and 2010 within the provision of advisory, legal and consultancy services.

In conformity with Article 5 (3) of the Free Access to Information Act, all the information provided was also published on the Office's website.



### **Annual Report Summary 2010**

The Office for Personal Data Protection

Pplk. Sochora 27, 170 00 Praha 7

E-mail: [posta@uouu.cz](mailto:posta@uouu.cz)

Web: [www.uouu.cz](http://www.uouu.cz)

In February 2011, Czech version of the Annual Report was published on the basis of duty imposed by article 29 (d) and 36 of the Act No. 101/2000 Coll., on the protection of personal data and of amendment to some acts.

Editor: PhDr. Hana Štěpánková, tel.: +420 234 665 286

Editorial revision: PhDr. David Pavlát

Graphic layout: Eva Lufferová