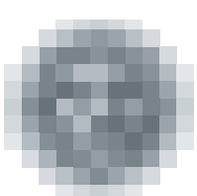
ANNUAL REPORT SUMMARY

2011



úřad pro ochranu
osobních údajů
the office for personal
data protection

The President of the Office looks back at 2011

The turning period for the Office for Personal Data Protection continued in 2011: On 1 June 2011, three new inspectors joined Ms Jana Rybínová and Mr Josef Vacula, who had been appointed for a ten-year term in August 2010: Mr František Bartoš, Mr Petr Krejčí and Mr Daniel Rovan. Ms Božena Čajková was elected as inspector for the second term. It is quite clear that the appointment of new inspectors was even more significant for the Office than the fact that it was entering a new decade of its work.

Although the new inspectors had to continue work on some of the difficult tasks that had been dealt with by their predecessors – such as monitoring and finalising the process of establishing the Prague Opencard system that would be issued without the processing of personal data (in this relation, the Office also addressed a considerable number of Prague citizens) – they soon also took on other important tasks: In my opinion, it is a genuine success that it was possible to establish a methodology for dealing with protection of the personal data of persons whose data are being processed without their consent, even though removal of such data can be requested only from webhosting service providers within the reach of European law.

Act No. 468/2011 Coll., amending, *inter alia*, Act No. 480/2004 Coll., on certain services of the information society and on amendment to certain laws, came into effect on 1 January 2011. This brought about various changes in the area of commercial communications and thus also in the competences conferred on the Office, which had duly prepared itself for this duty at the end of the year.

The strong interest of the Office in disseminating knowledge on personal data protection was clearly visible last year. This is witnessed by the number of workshops and conferences held both in this country and abroad that were attended by experts of the Office, as indicated in the relevant chapters of this Annual Report. I must also mention the co-operation of the Czech Office with its partners in Poland and Hungary. Through our joint efforts, we managed to create a special publication that helps entrepreneurs find their way through the conundrum of legal regulations relating to protection of personal data in these countries as well as throughout Europe. Thus, this guide justifiably caught the attention of both the European Commission and the Council of Europe.

It is certainly worth noting that in December of last year, the Office issued the 60th volume of its Official Journal, where it introduced the fundamental legal documents concerning personal data protection of pan-European scope and legal opinions of the Office on matters that it is required to resolve within the Czech legislation.

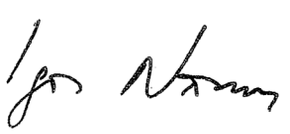
In two issues of its Information Bulletin, the Office presented the general public with various ways of viewing the situation drawing attention to two aspects that would deserve special legislative regulation in the viewpoint of the Office: utilisation of genetic data and processing of DNA data and – as an issue of similar importance – the use of cameras and video surveillance systems, which lacks a comprehensive legal basis. Of course, I appreciate the fact that the media showed great interest in the use of video surveillance systems.

In the context of the difficult economic situation, the Office has also been able to deal with financial and staff requirements ensuing from its new competences. So far, it has managed to fully perform all the duties required of the Office in relation to electronisation of public administration, and has also achieved the necessary progress in building the so-called ORG system, which was entrusted to it within e-Government.

I would like to see the same attention and care devoted to personal data protection in the legislative process. We have been taking all the steps allowed by our legislation in this respect and I believe that protection of privacy will receive adequate attention and care particularly in the coming era and boom of "cloud" systems.

At the end of the year, the Office began creating preconditions for the successful performance of its duty in the area of "**data breaches**", where new European regulations explicitly afford the service providers of electronic communications an innovative instrument for the protection of personal data and privacy; in the Czech Republic, these regulations were implemented by amending three different laws – the Electronic Communications Act, the Personal Data Protection Act and the Information Society Services Act – effective from 1 January 2012.

Although it is difficult to estimate the scope of duties ensuing from this task, I view next year with optimism. This is so particularly because, after having served for seven years as the President of the Office and on the basis of my interactions with its employees, and also in view of my experience with the substantially renewed board of inspectors, I know that we have so far been able to successfully resolve all of our complex and time-demanding tasks. I am sure that this allows me to look to 2012 at least without trepidation.



Igor Němec

Contents

Office in numbers 2011

Inquiries and consultations	inquiries in the Czech Republic	2294
	abroad	110
	consultations	
	for state administration	104
	for local governments	160
	for legal persons	301
	for natural persons operating a business	216
	for natural persons	1544
Pleadings and complaints	instigations received pursuant to the Personal Data Protection Act	1119
	complaints referred for inspection	197
Unsolicited commercial communications (competence pursuant to Act No. 480/2004 Coll.)	total instigations	4613
	instigations resolved	2283
	inspections initiated	157
	inspections completed	137
	administrative decisions on a fine	63
Inspections (excluding inspections concerning Act No. 480/2004 Coll.)	initiated	179
	completed	144
	referred to other governmental authorities	1
	challenged by objections	25
	objections accepted	9
	objections dismissed	9
	mostly accepted	1
	mostly dismissed	4
Administrative punishment	administrative proceedings for violation of Acts No. 101/2000 Coll. and No. 133/2000 Coll.	110
	infraction proceedings pursuant to Act No. 101/2000 Coll.	16
	administrative and infraction proceedings pursuant to Act No. 101/2000 Coll. - Articles 44a and 45a	5
	infraction proceedings for violation of Act No. 159/2006 Coll., on conflict of interests	1
	appealed decisions on violation of law	49
	(*NB: ** of which in respect of Article 17*)	(2**)
	appeals dismissed	25

	cancelled and returned for new hearing	8
	cancelled decisions and proceedings discontinued	10
	change in the decision	5
Judicial review *(NB: ** in total since 2001)*	court actions lodged	10 (91**)
	actions dismissed by the court	4
	decisions cancelled by the court	5
	referred for a decision (pursuant to Article 21 of Act No. 101/2000 Coll.)	0
	court proceedings closed / pending	1/9 (50/41**)
Registration	notifications received (pursuant to Article 16 of Act No. 101/2000 Coll.)	4421
	instances of processing registered	3856
	still pending	953
	registrations cancelled	49
	notifications on a change in the processing	866
	proceedings pursuant to Article 17	82
	discontinued (no violation)	68
	discontinued for procedural reasons (e.g. notifications withdrawn)	8
	not permitted	6
Authorizations for transfers of personal data abroad	applications for transfer of personal data abroad received (pursuant to Article 27 of Act No. 101/2000 Coll.)	9
	decisions on authorisation of transfers	3
	decisions on dismissal	0
	proceedings discontinued for procedural reasons	6
Complaints pursuant to Article 175 of the Code of Administrative Procedure	complaints received	28
	complaints found justified	5
	complaints found partly justified	9
	complaints found unjustified	17
Applications pursuant to Act No. 106/1999 Coll.	applications received	23
	applications resolved	21
	applications rejected	2
Materials published	Official Journal (number of volumes)	3
	Information Bulletin (number of volumes)	2
Press conferences	regular	3
	extraordinary	0
Legislative drafts on which comments were made	laws	75
	implementing regulations	91
	draft government regulations	21
	draft decrees	70
	other	51
	foreign materials	29

Investigation activities of the Office

2011 INVESTIGATION PLAN

I. GENERAL TOPICS FOR SPECIFICATION OF THE INSPECTION ACTIVITIES PURSUED BY INSPECTORS OF THE OFFICE

1. PUBLIC ADMINISTRATION INFORMATION SYSTEMS

1.1. The global census took place in 2011 together with collection of the related information. The Office took part in preparation of the conditions for this major data processing exercise and monitored the census including the related processing of statistical information in conformity with Act No. 296/2009 Coll. and the implementing regulations. With a view of fulfilling this task, an inspector of the Office commenced an inspection of the Czech Statistical Office, focusing particularly on complaints lodged by persons involved in the census and related, not only to the census as such, but particularly to filing of anonymised forms in the National Archives and the results of the census at the Statistical Office. The inspection was initiated on 2 June 2011 and has not been completed yet.

1.2. In respect of the dynamically developing issue of electronic communications in the area of PAIS (Public Administration Information Systems), the Office focused on the level of security guaranteed for electronic acts performed by the public authorities through data boxes operated within the data box information system in conformity with Act No. 300/2008 Coll., on electronic acts and authorised conversion, as amended.
With a view of performing this task, an inspector of the Office commenced an inspection of the Ministry of the Interior as the controller and the Czech Post as the operator of this system. It was subsequently found necessary to extend this inspection to another entity, specifically the Ministry of Justice.
The results of the inspection are published in the chapter Control of court documents delivery via data boxes.

1.3. In accordance with the obligations of the Czech Republic in the area of the EU Third pillar, including the Schengen Convention, and in view of the upcoming evaluation of compliance with these obligations, it is anticipated that regular inspections will be carried out at some of the obliged entities.

Several supervisory activities were carried out with a view of fulfilling this task, focusing on the pursuit of visa and other consular activities by a number of embassies. All these inspections, which were concerned with the security afforded to the personal data of visa applicants and their right to information, will yield common conclusions that will be discussed with the Ministry of Foreign Affairs.

An inspection at the Czech embassy in Mexico was performed on 3 November 2011 and another inspection at the embassy in Macedonia took place a week later; an inspection of the embassy in Moldova was carried out on 6-8 December 2011.

Another inspection in this area was concerned with the EURODAC information system. As the inspection activities in the Schengen Area were found to be rather premature in view of the coming events (an evaluation mission will take place in the Czech Republic in 2012 and the Office will present its results together with other partners in this area), the inspection was postponed to the following year. The inspection will be concerned with a number of entities, specifically the Ministry of the Interior, the Ministry of Justice and the Ministry of Foreign Affairs.

By contrast, an inspection of the Schengen Information System (SIS) has been launched including control of logged access to the system. Emphasis is placed in this control on checking the application of Art. 96 of the Convention implementing the Schengen Agreement concerning the entry of foreigners' personal data in the SIS in case of serious breach of public policy and security of the state.

1.4. In view of the growing requirements and demands of the operators of integrated security and transport systems utilising technical options for performing their duties, it is in the interest of the Office to verify compliance with the duties of these entities in relation to personal data protection.

With a view of fulfilling this task, an inspector of the Office performed inspection of the system of multifunctional cards in the public transit system operated by the Statutory City of Plzeň. The inspection was carried out in the period from February to March 2011 and did not reveal any shortcomings.

1.5. Another inspection following from the inspection plan was concerned with compliance with the controller's duties in the processing of the personal data of clients and their family members in a selected facility in relation to the provision of services in the area of social care. With a view of performing this task, the authorised inspector commenced the inspection of the selected entity in November 2011.

2. INFORMATION SYSTEMS IN THE AREA OF PRIVATE LAW

Based on the latest findings and experience, the Office's inspection activities in this area were focused on:

2.1. Conditions of personal data processing in relation to the issue of customer fidelity cards for all types of services with a focus on compliance with the duties of the responsible persons in the collection of this information directly from the individual entities.

In the period from February to August 2011, an inspector of the Office carried out inspection at the dm drogerie markt, s.r.o. concerned with personal data processing in relation to issuing and using customer cards. Although the inspection did not reveal any substantial shortcomings in the processing of the customer data, based on the inspector's recommendation, the controlled entity changed its practice in collecting and maintaining copies of documents declaring the customers' claims for the provided benefits and discounts on goods.

This area was also in the focus of the inspector who, in the period from February to May, performed an inspection at BAUMAX ČR, s.r.o. concerned with processing of customer data through a customer card. This inspection did not reveal any violation of Act No. 101/2000 Coll., on personal data protection, as amended (hereinafter the "Personal Data Protection Act").

Personal data processing related to the use of customer cards was also the subject of an inspection initiated in February 2011 at the pharmaceutical company Česká lékárna, a.s. This control is still underway and expected to be completed in January 2012.

2.2. Conditions of processing of passenger data in the context of video surveillance systems operated in public transport means.

With a view of fulfilling this task, an inspector of the Office performed an inspection of the Public Transport Company of the City of Ostrava in September and October of 2011. The inspection was closed without ascertaining any breach of the duties of the controlled entity, as no processing of information of concern was carried out at the time of the inspection.

2.3. Conditions of processing of patient data in the the information systems of entities providing health care services.

With a view of fulfilling this task foreseen in the inspection plan, in October 2011, an inspector of the Office initiated an inspection at the Na Homolce hospital, which is a state-funded institution. The inspection was closed in January 2012 only to find out that the controlled entity had not breached the duties of a data controller in the course of the usage of registration bracelets.

2.4. Conditions of processing of customer data in offering goods and services, not only within the Personal Data Protection Act, but also in other areas of the Office´s competence in respect of the information society services in the sense of Act No. 480/2004 Coll., on certain services of the information society, as amended.

In order to fulfil the task of checking the processing of the customer data and other persons´ data in relation to marketing services, an inspector of the Office initiated an inspection at Alza.cz. This inspection was carried out in collaboration with the Slovak Office for Personal Data Protection; however, this was later found to be a demanding task in view of the extensive network of services provided by the controlled entity. The inspection still has to be completed by January 2012 expectedly.

2.5. Conditions of personal data processing in relation to pursuit of the activities of a private security agency or private detective agency.

With a view of fulfilling the task of checking the duties of the controller and processor in relation to monitoring of visitors to sports events and in the pursuit of the activities of a private security agency, an inspector of the Office initiated an inspection of the Teplice Football Club. The inspection was closed without finding any breach of the data controller's duties in processing of personal data. The inspector concluded that the

responsible entity processed the personal data of visitors to the stadium by virtue of a video surveillance system operated by the municipal police. It was not found that the controlled entity would process personal data of visitors in relation to the purchase of tickets to the stadium.

3. PROCESSING AND DISCLOSURE OF PERSONAL DATA IN THE AREA OF CRIME PREVENTION AND FIGHT AGAINST TERRORISM

Based on the applicable legal regulation of the conditions for the retention of data created or processed in relation to the publicly accessible services of electronic communications or public communication networks, it was found necessary to perform the following:

3.1. Control of compliance with the rules for disclosure of traffic data in telephony and e-communications in conformity with the Directive 2006/24/EC
In view of the envisaged new legal regulation of these conditions, this project was postponed to 2012.

3.2. Control of compliance with the conditions for personal data processing in a situation where the controller and processor have entered into agreement on processing of information pursuant to Article 6 of the Personal Data Protection Act
Inspectors of the Office commenced an inspection of the integrated municipal video surveillance system in Prague (the controlled entity being the Prague City Hall). `
This project is also aimed at fulfilling the task pursuant to section 2.2. This inspection is still underway and will be completed in March 2012.

II. INSPECTIONS INITIATED IN 2011 ON THE BASIS OF AN INSTIGATION OF THE PRESIDENT

As in previous years, in 2011 the President of the Office again used the option of instructing certain inspectors of the Office to perform an inspection, particularly in respect of cases of general importance calling for urgent action.
The President gave the following instructions in 2011:

1. An instruction to perform control at the Ministry of Justice on the basis of which the given inspector initiated an inspection on 25 January 2011. Based on information published by the media and the Ministry of Justice, it was clear that, within publication of the documents entitled "List of judges – former members of the Communist Party" on the website at www.justice.cz, the Ministry disclosed inaccurate personal data on membership of certain judges and state attorneys in the former Communist Party of Czechoslovakia. This conduct could have resulted in violation, particularly of Article 5 (1) (c), Article 5 (2) and also other provisions of the Personal Data Protection Act. The inspection was completed by imposing a fine of CZK 100 thousand, which was paid by the controlled entity.

2. An instruction to perform inspection of Telefónica O2 Czech Republic, a.s., which was carried out by the authorised inspector in May 2011. The instruction was issued in relation to the published information concerning surveillance of a manager of the ČEZ

power company, indicating a suspicion of violation of the Personal Data Protection Act. No breach of duties by Telefónica O2 Czech Republic, a.s. was ascertained.

3. An instruction to inspect the Embassy of the Czech Republic in Mexico, which was performed by the authorised inspector in October 2011. The requirement for this inspection resulting from the Schengen evaluation is contained in the general part of the inspection plan of the Office for 2011. Fulfilment of this task was an important step towards successful Schengen evaluation and performance of the obligations arising for the Office in relation to this evaluation. The results will be presented during the European supervisory mission of the Schengen system in February 2012.

4. An instruction to perform inspection at the administration of the Central Bohemian Region. Based on information available from public sources, the Office came to the conclusion that it would be necessary to initiate an inspection of processing of personal data of persons applying to the Central Bohemian Region for the provision of a special purpose donation for the payment of regulatory fees in health-care facilities. Publication of personal data on the website of the Central Bohemian Region gave rise to a suspicion that this conduct could constitute breach of the duties stipulated by the Personal Data Protection Act, particularly by Article 5 (1) (f) of the Act, by the mentioned entity. The inspection has not been completed yet.

5. An instruction to perform an inspection at Městský dopravní podnik Opava, a.s. (the Opava City Transport Company). The instruction was issued in relation to the previous instigations from the Sectoral Union of Employees in Transport, Road Management and Car Repairs of Bohemia and Moravia, which were concerned with stating the names and surnames of bus drivers in the public transit system on tickets, and also based on an instigation from the representative of the Public Defender of Rights (the Ombudsman), who addressed the Office through a letter of 19 September 2011 in the same matter. Theinspection focused on compliance with the duties of a data controller following from thePersonal Data Protection Act, particularly from Article 5 (1) and (2) and Article 10 of the Act. By processing the personal data of its employees – bus drivers – within the scope of their name, surname and personal number, by means of printing this information on the tickets without the consent of the data subject, the Opava City Transport Company breached the duty of a personal data controller imposed by Article 5 (1) (d) and Article 5 (2) of the Personal Data Protection Act. At the same time, the controlled company was required to take a remedial measure – to stop processing personal data of its employees – bus drivers – by printing their name, surname and personal number of the tickets sold in the bus.

6. An instruction to check the authorisation of the Municipal Court in Prague to process personal data, which was assessed by the complainant as a possible breach of the duties of a data controller under the Personal Data Protection Act. The inspection is underway; the inspection protocol should be drawn up by mid-February 2012.

7. An instruction to check the manner of transferring personal data processed by Vodafone Czech Republic a.s. to the register of debtors kept by the SOLUS company. The instruction was addressed to an inspector of the Office, where the inspection was to focus both on Vodafone and on SOLUS. Following analysis of the related facts, the inspection was not initiated and the instruction was forwarded to the administrative activities department

with a view of initiating administrative proceedings. Detailed information is published in this Annual Report in the chapter Findings obtained in administrative proceedings.

8. An instruction to perform an inspection at the Kuřim Municipal Authority. The instigation was concerned with determination of the property of applicants for one-off contributions for the purchase of special aids pursuant to Article 33 of Decree No. 182/1991 Coll. An inspector was commissioned to check compliance with the duties of all the responsible entities pursuant to the Personal Data Protection Act in relation to application of the conditions for granting social care benefits. The inspection was closed on 4 August 2011 with a statement of violation of the Personal Data Protection Act and the case was submitted to the relevant department to open an administrative proceedings.

9. An instruction to inspect the District Court in the town of Teplice in respect of operation of data boxes, and liability for incorrect delivery of court documents to the data box of an entity that was not a party to the proceedings. The Office was requested by the Public Defender of Rights to exercise its supervisory powers. The instigation was made with a view of checking compliance with the duties of the responsible entities pursuant to the Personal Data Protection Act in relation to sending messages through the data boxes information system, and particularly in relation to unambiguous identification of the recipients of these messages. The results of the inspection are published in the chapter Control of court documents delivery via data boxes.

FINDINGS OBTAINED BY INSPECTORS FROM INSPECTION ACTIVITIES

CONTROL OF COURT DOCUMENTS DELIVERY VIA DATA BOXES

The number of complaints increased in 2010 and 2011 in respect of the delivery of court documents addressed to attorneys-at-law to the data boxes of natural persons operating a business. It followed from a statement of the Ministry of Justice that documents had been erroneously served by a number of courts; this followed from the results of investigation pursued by the supplier of information systems. In addition, the Ministry of Justice also records individual complaints.

On the basis of this information, an inspection was initiated in conformity with the Office's plan of inspection activities. The inspection was concerned particularly with the system conditions created for the performance of the administrators' duties in processing personal data within ISDS (Data Boxes Information System), with special emphasis on the performance of duties in securing personal data as stipulated in Article 13 of the Personal Data Protection Act.

In view of the fact that the main objective of an inspection is to provide for a remedy and create system conditions for eliminating human errors, three local investigations were performed in respect of the responsible employees of the Ministry of Interior, which

establishes and administers the data boxes. Employees of the Ministry of Justice were also invited to the last investigation, particularly because all the complaints were concerned with courts.

According to statements made by the representatives of both ministries, a separate flag should be introduced for attorneys-at-law as from the date when data boxes will be compulsorily established for attorneys, i.e. from 1 July 2012.

PERSONAL DATA IN HEALTH CARE

An incidental inspection was carried out in the area of protection of personal data in health care at the instigation of one patient. While the suspicion of loss of documents was not confirmed, the records of loaned medical cards and handover of copies of the contents of the cards were kept inadequately. A measure was imposed within the inspection, where the given entity was required to keep duplicate records of loans outside the medical documents with a view to preventing similar cases.

PERSONAL DATA IN INSURANCE INDUSTRY (HEALTH INSURANCE)

A change in the patients' registration – transfer to a different health insurance company without their knowledge was the subject of several inspections.

Within inspection of one of the health insurance companies, it was ascertained that the insurance company entered into agency contracts with external entities with a view to obtain new clients. However, the agents also had access to the auxiliary software. At the time of the inspection, the health insurance company kept up-to-date records of fraudulent conduct related to false applications for health insurance and had registered a total of 100 cases of fraudulent conduct that had been investigated by the Police of the Czech Republic. According to the findings of the Office, false applications were submitted to the insurance company with which the agent had entered into an agency contract.

Another case of fraud involving applications for health insurance was also recorded by the Police of the Czech Republic. Personal data of allegedly "insured persons" had probably been obtained from contracts concluded by these persons, e.g. with telecommunication companies, in which the agent had also been involved, or contracts encountered by the agent in his work. The agent thus counterfeited applications for health insurance in a total of 47 cases.

The inspection was closed with the conclusion that the health insurance company itself had not violated the Personal Data Protection Act. However, in the inspection protocol, the inspector noted that the criminal aspects related to seeking new clients should be dealt with by the insurance company particularly through preventive measures, specifically by introducing effective control mechanisms. Before entering a newly insured client in the database, the insurance company should verify whether the personal data of the insured person, including his/her signature on the application, correspond to the facts.

Another inspection was initiated on the basis of a complaint received by the Office through the Office of the Public Defender of Rights (the Ombudsman). On the basis of this complaint, an inspection was carried out in a health insurance company with which the complainant had

been newly registered without her knowledge. The health insurance company terminated co-operation with the employee who had actually carried out the registration.

In respect of this issue, it must be stated that the patient's right to a change of health insurance company was regulated at the time when these inspections were carried out by Act No. 48/1997 Coll., on public health insurance, as amended. According to Article 11 (1) (a), the insured person had the right to choose his/her health insurance company. A person could change his health insurance company once every 12 months, in each case as of the 1st day of a calendar quarter.

An amendment to Act No. 48/1997 Coll., on public health insurance, entered into force on 1 December 2011, including modification of Article 11 (1) (a): An insured person has the right to choose his/her health insurance company unless this Act stipulates otherwise. However, the health insurance company may be changed only once every 12 months, in each case as of 1 January of the subsequent calendar year; the insured person or his/her legal representative must submit the application to the selected health insurance company not later than 6 months before the requested date of the change.

In another case, the Police of the Czech Republic referred to the Office an instigation concerned with a suspicion of possible leakage of information related to unauthorised access to a physician's e-mail box.

The Police of the Czech Republic stated that as a result of inadequately securing access to his e-mail box, the physician could have enabled access to sensitive data concerning the state of health of his patients, thus violating the Personal Data Protection Act.

The Office's investigation did not prove any serious misuse of the personal data that were allegedly stored in the physician's e-mail box. In a letter addressed to the Office, the Police of the Czech Republic subsequently stated that it was still investigating whether the physician's e-mail box had indeed been accessed without authorisation. Based on the investigation, the inspector came to the conclusion that the Personal Data Protection Act had not been violated in relation to the physician's suspicion of misuse of the personal data stored in his e-mail box and the inspector therefore suggested that the instigation be dismissed.

MEANS-TESTING OF APPLICANTS FOR ONE-OFF CONTRIBUTIONS FOR THE PURCHASE OF SPECIAL AIDS FOR HANDICAPPED CITIZENS

The Public Defender of Rights addressed the President of the Office with a request for collaboration in investigating an instigation made by a complainant which was concerned with determination of the income and property (means-testing) of applicants for one-off contributions for the purchase of special aids for handicapped citizens according to Decree No. 182/1991 Coll., implementing the Social Security Act and the Czech National Council Act on the Competence of Authorities of the Czech Republic in Social Security. He stated that he had investigated into the procedure of a municipal authority with a view to check the practice in determining the social and property situation of applicants for one-off contributions for the purchase of special aids. In this investigation, the Defender established that the authority ascertained the said facts although these facts were not a criterion for the existence of entitlement to the benefit and determination of its amount.

An inspector of the Office for Personal Data Protection initiated an inspection of the municipal authority in relation to the processing of personal data of the applicants in assessing and granting a one-off contribution for the purchase of special aids according to the Decree of the Ministry of Labour and Social Affairs.

In the inspection, it was determined that in assessing and granting the one-off contribution for the purchase of special aids according to the Decree, the municipal authority determined the income and property of the applicants and of persons assessed jointly with the applicants as a basis for its administrative decision (in respect of jointly assessed persons, it also collected other personal data, specifically their name, surname, date of birth, birth identification number, employment). The necessary scope is stipulated by the cited legal regulation, which does not provide for the duty to ascertain, collect and maintain personal data on the income and property of the applicants for the contribution or other persons (spouse, common-law partner) in proceedings on the provision of a one-off contribution for the purchase of special aids. If the aforementioned personal data are not necessary for the proceedings, they cannot be processed even with the consent of the applicant pursuant to the Personal Data Protection Act, because such consent cannot put right misconduct of the State administration that is governed by special legal regulations and, **according to the current legal regulation, it is not permissible to collect the personal data of applicants for a social benefit to an extent exceeding the scope permitted by the said special legal regulations**.

INSPECTION OF THE COMMERCIAL REGISTER

(Electronic form of the Commercial Register available at www.justice.cz.)

The web portal of the Commercial Register is an important public information system whose significance is reconfirmed by its importance for e-Government. Personal data are processed on the Internet via this portal. The Ministry of Justice is the data controller in this instance. The Ministry is therefore responsible for ensuring that the scope of the published data and the period of time for which the data are published correspond to the purpose of processing.

USE OF BIRTH NUMBERS IN PUBLIC ADMINISTRATION

Pursuant to Article 13c of Act No. 133/2000 Coll., on records of the population and birth numbers and on amendment to some laws, as amended, both local governments and governmental authorities may use birth numbers in those cases where they are explicitly authorised to do so by the Municipalities Act and other special laws. However, they may use birth numbers only for the given purpose stipulated by the law and for no other purpose. In other cases, e.g. in providing donations and scholarships, organising social events, publishing candidates, etc., neither the public administration nor any other organisation is authorised to use birth numbers for database search.

PERSONAL DATA OF EMPLOYEES

The Office has repeatedly encountered a situation where the employer requests personal data from job applicants, where it is impossible or very difficult to find any appropriate legal basis for collection and further processing of these data. This usually occurs within negotiations on establishing the employment relationship, i.e. before a decision on employment is actually made. The employers then justify the requests for such personal data by the nature of the future job. This includes, for example, information on incapacity for work during the past year, personal status or the number of children, whether or not the applicant smokes, without the job seeker being informed about the processing of personal data in relation to the selection and hiring new employees pursuant to Article 11 (1) and (2) of the Personal Data Protection Act. Such requests for personal data are at strict variance with the Labour Code.

PERSONAL DATA IN THE CONTEXT OF GENERAL TERMS AND CONDITIONS

Personal data of consumers are processed in relation to a number of contractual relationships, particularly "consumer contracts" concluded between a supplier and a consumer. The supplier (entrepreneur) provides certain services or goods, for which he utilises the consumer data and thus assumes the position of a data controller; the consumer, if he is a natural person, is in the position of the data subject.

The Office has been dealing with the issue related to the aforementioned relationship in terms of the Personal Data Protection Act for a long time and repeatedly; consequently, in August 2011, it issued Position No. 2/2011, in which it expressed its legal opinion on personal data processing conditional on consent incorporated in a contract or in General Terms and Conditions (hereinafter "Terms and Conditions").

It is logical that in a number of cases, an entrepreneur needs to identify his client so that he is able to conclude a valid contract and that he needs to know the client's identification details to be able to properly perform the contract, i.e. deliver the goods, provide the service, etc. Consequently, processing of personal data for the purpose of concluding a contract is not conditioned by the data subject´s consent and the Personal Data Protection Act therefore envisages these cases and does not require redundant consent for the purpose of the actual conclusion of the contract.

On the basis of the law, the client's consent is a free and informed manifestation of will. "Free" means that the decision of the data subject does not have effect on the other terms and conditions. "Informed" means that the client is aware what he actually gives consent to and what consequences could ensue from this.

The first condition unambiguously means the possibility of choice, i.e. that rejection of the consent must not be a fact preventing the establishment of the legal relationship. Indeed, it is the informed nature of the consent that is highly questionable within Terms and Conditions. The client usually wants to conclude the contract (he needs to borrow money, wants a new telephone, etc.) and, in this situation, he is inclined to execute a concise and transparent contract, while not paying enough attention to the Terms and Conditions, particularly given their scope and format.

While in view of the law, the service provider has formally performed his statutory duties, in actual fact the existence of a fully-fledged informed consent could be successfully doubted.

In this respect, it should be noted that the Office constantly encounters cases where the Terms and Conditions include provisions on consent to personal data processing with a view to concluding and performing the contract, and even make the contractual relationship conditional on the existence of this consent. Such provisions are misleading for the client. The fact that the client may revoke the consent changes nothing in the fact that the entrepreneur can continue processing the client's personal data without his consent.

The Office can deal with this inappropriate practice both by exerting pressure on the service providers to incorporate the consent in the contract itself or at least highlight the relevant passage in the Terms and Conditions, and by raising the awareness of the data subjects aimed at their increased competence in this area.

A manifestation of will to the effect that the client does not intend to provide consent to processing his personal data can be recorded in several ways. In a case where the contract is being concluded in writing, the client may either cross out the specific provision on consent in the Terms and Conditions or attach a note to this provision (or make such a note at some other suitable place in the contract) that will clearly express his will (e.g. "I disagree with processing of personal data for marketing purposes"). It is then the duty of the controller to respect this manifestation of will and not to make the establishment of the contractual relationship conditional on (i.e. enforce) granting the consent. If the client concludes a contract with the thus-modified Terms and Conditions, it means that he did not grant consent to processing of personal data to the controller.

It is very important for the client to know that if he grants consent during conclusion of the contract, nothing prevents him from revoking the consent after the execution of the contract if he comes to the conclusion that he no longer wishes that his personal data be processed. For this reason alone, the controller's requirement for consent in conclusion of contracts is unnecessary.

However, realistically, the standard procedures of major companies in relation to minor clients encompass pressure against these clients and they often take advantage of the fact that the clients are not actually aware of the possible consequences resulting from a blank consent.

Another form of pressure exerted on the client within the Terms and Conditions consists in the mentioned consent to the provision of his personal data to other entities within a certain "alliance" of the given companies, which however need not interest the client at all. The actual purpose of this consent lies, of course, in marketing measures and commercial communications.

Furthermore, within the Terms and Conditions, the data subjects give their consent to the fact that their personal data including their birth identification number will be provided to members of the provider, and the client again signs that he gives this consent voluntarily.

It is absolutely common that the part of the Terms and Conditions concerned with the consent also includes a paragraph related to monitoring of the client's communication, where monitoring means particularly recording of voice communication or data correspondence.

There are also Terms and Conditions in which the client approves that the contractual partner will process the client's personal data for the purposes of offering trade and services also after the rights and obligations under the contract have been settled, i.e. after termination of the contractual relationship.

For the clients, it is very important to know that they may refuse the consent. In practical terms, it is therefore entirely up to the client whether or not he agrees with the part of the Terms and Conditions comprising the consent to processing of personal data by concluding the contract as presented. As a matter of principle, the Terms and Conditions are unfavourable for the data subjects. The mutual contact is shifted from a direct dialogue between contractual partners to a duty to provide information. For the client, this means that the service provider supplies him with information via the provider's website, which a common customer may not even notice. This form allows major companies to communicate "collectively", rather than individually, with a number of small clients, thus relieving them from a major part of their responsibility.

In cases of application of Terms and Conditions to the area of personal data processing, it must be distinguished where consent is required for personal data processing (marketing, registers of debtors, etc.) and where consent is not necessary (conclusion and performance of the contract, enforcement of receivables under the contract). The formulation of the consent and the possible performance of the information duty should then be adapted to these cases. Where consent is provided, it is necessary to allow the data subject to express his will and respect this expression of will so that it constitutes free and voluntary consent to personal data processing. Separately formulated parts of the Terms and Conditions with boxes to be checked by the data subject to express their consent can be recommended as the most suitable method. If consent is included directly in the text of the Terms and Conditions, the controller must respect that the data subject crosses-out these parts of the Terms and Conditions. For transfer of personal data to third parties, the data subject must first be informed of the purpose of processing by the third party and of identification of this party.

In general, it must be noted that the principle of conclusion of contracts including Terms and Conditions is unsuitable for minor clients. At the given time, the data subject is unable to properly examine all the terms and conditions of the mutual relationship or even consult an expert. He is under indirect time pressure, which in combination with the extent of the presented text does not allow him to become properly acquainted with the entire contents of the contract. While this procedure employed by certain major companies is not at variance with the law, it is not entirely honest to the minor client.

DEBT COLLECTING COMPANIES, PARTICULARLY THOSE OPERATING VIA INTERNET

Based on a questionnaire filled-in by the creditor, where the creditor identifies his debtor, a contract of mandate is executed or a power of attorney granted for enforcing the creditor's claim. On the basis of this contract or power, the company then attempts to enforce the debt, together with a certain surplus as its fee.

In terms of personal data protection, it is questionable as to what legal title could form a basis for processing of the personal data of the debtors.

It must be noted that debt collecting (enforcement) companies exert pressure on the debtors by invoking the possibility of including them in the "public register of debtors", which is available to anyone on the Internet. This procedure has no legal basis, as the debtor's consent is clearly missing. These cases often infringe on the personal rights of these persons, because the enforcement company often unjustifiably identifies a person who owes nothing

to anyone as a debtor simply by including this person in the register of debtors. Indeed, (s)he may not even become aware of the fact that (s)he has been published as a debtor.

PERSONAL DATA PROCESSING THROUGH VIDEO SURVEILLANCE SYSTEMS

The number of pleadings concerned with the operators of video surveillance systems received in 2011 was comparable to the number in 2010. Of the total number of 375 pleadings, almost 90 % were concerned with the surveillance of employees at workplace or the operation of video surveillance systems in apartment and private buildings. It can thus be summarised that although absolute generalisation would be misleading, a majority of citizens have more or less come to terms with cameras, e.g. at airports, in the metro and at banks, but are still highly sensitive to any infringement of their privacy, particularly at workplace and at home. When dealing with the use of cameras fitted with a recording device at workplaces, the Office has long been co-operating with the area labour inspectorates, because the use of such systems violates primarily Article 316 of the Labour Code.

Pursuant to Article 3 (3), the Personal Data Protection Act does not apply to personal data processing that is performed by a natural person exclusively for his or her personal needs. The use of video surveillance systems for the protection of citizens' own property, mostly private homes, is a typical example.

Hundreds of pleadings concerned with the operators of video surveillance systems that were received in 2011 indicate that the most frequent breaches of the duties imposed by the Personal Data Protection Act were as follows:

- misuse of the recorded images for other than declared purposes;
- disclosure or publication of the camera images (footage) to unauthorised persons;
- failure to adopt appropriate technical and organisational measures minimising the risk of unauthorised access to the camera recordings;
- excess of the principles of proportionality between the protected interest (objective) and interference with the privacy of natural persons;
- failure to perform the information and notification duties.

DISCLOSURE OF VIDEO RECORDINGS OF MUNICIPAL ASSEMBLY MEETINGS

Both general public and journalists paid close attention in 2011 to the issue of making and subsequent disclosure of video recordings of the meetings of a municipal assembly.

A municipality must clearly specify the purpose of acquiring an audio or video recording of a meeting of its assembly. If the assembly resolves to make a recording in that the entire agenda of the meeting is recorded authentically without any modifications, this constitutes creation of a document that is subject to the provisions of Act No. 499/2004 Coll., on archives and the filing service.

If the municipality opts for a live broadcast from the meeting without making a recording, this does not constitute collecting of personal data and such on-line broadcast is not subject to the provisions of the Personal Data Protection Act (Position of the Office No. 1/2006).

If the making of the video recording is aimed at preparing a TV newscast that will inform the citizens about the activities of the assembly without simultaneously presenting personal data, this is not a document, but rather only a newscast, which is governed by the provisions of Act No. 40/1964 Coll., the Civil Code.

If the municipality decides to make **live broadcasts** from the meetings of its assembly, it should meet several conditions:

1) The decision of the assembly to provide an on-line broadcast should be approved by a resolution of the assembly (setting the purpose of personal data processing).
2) The manner and means of the on-line broadcast (location of cameras, range of the cameras, etc.) from the meeting should be stipulated in the rules of procedure of the assembly.
3) Anyone who attends such a meeting should be informed in advance of this fact and also on accessibility of this broadcast (via the Internet without limitation or with limited access, CCTV or cable television).

However, it must be noted that there exists no legal basis that would unambiguously support the legitimity of processing of information from meetings of municipal assemblies with the use of modern audiovisual equipment and the Internet.

The results of inspection activities of the Office clearly indicate the **need for adopting legislative measures** that would deal or further specify, among other things, the subject of live broadcasts and making video and audio recordings of the meetings of elected bodies, i.e. an amendment to the laws on municipalities, regions and the Capital City of Prague.

INSUFFICIENT SECURING OF PERSONAL DATA (ARTICLE 13 OF THE PERSONAL DATA PROTECTION ACT)

Most frequent shortcomings established in 2011 and in the previous years in the Office's supervisory activities concerned with compliance with Article 13 of the Personal Data Protection Act.

Article 13 of the Personal Data Protection Act on securing personal data is, in substance, very strict, because it stipulates that *it is necessary to adopt measures preventing unauthorised or accidental access to personal data*. Implicitly, by contrast, if such access was gained, the measures were insufficient.

An amendment to the Personal Data Protection Act adopted in 2007 further specified the concept of authorised persons: The data controller is obliged *"to ensure that natural persons authorised to use the systems for automated processing of personal data have access only to the personal data corresponding to the authorisations of these persons, based on special user authorisations established exclusively for these persons"*.

Systems for automated personal data processing pursuant to the Personal Data Protection Act may be used only by authorised persons; natural persons authorised to use the systems for automated processing of personal data shall have access only to the personal data corresponding to the authorisations of these persons according to special user authorisations established exclusively for these persons, and particularly functions must be set for the acquisition *of electronic records that will enable to determine and verify when, by whom and for what reason personal data were recorded or otherwise processed*.

The Office focused its inspection activities on the government, specifically on the public register published at www.justice.cz and on the register of the State Environmental Fund. The Office requested that the existence of such a register be always perceived as personal data processing, because this is what actually occurs in these registers, and therefore that there always be a clearly identified controller who performs the duties under the Personal Data Protection Act. In general, it must always be considered whether and what personal data may be published on the Internet: if this is a statutory duty, the law should clearly stipulate what exactly is to be published.

In instances involving storage of camera recordings made with a view to protecting property and detecting crime, the Office requires that these recordings be secured so that they can be perused only after an incident has occurred. At most, the Office permits an exemption for the security director who controls suspicious persons, e.g. in art galleries. However, in any case, it is necessary that the given person log in with specification of exact data on the purpose of inspection. Recordings of security cameras may not be used for any other purpose. These recordings may in no case be provided to the media (TV) or the police, unless the latter have commenced investigation.

Pseudoanonymous data are data that have allegedly been rendered anonymous, e.g. by omitting the surname and birth identification number, while maintaining other data allowing for identification of a certain person. However, it must always be borne in mind that anonymisation is a process that provides not even an indirect possibility of identifying the given person.

THE "MUZZLE ACT"

(Compliance with Articles 8a to 8c of Act No. 141/1961 Coll., on criminal court proceedings - the Code of Criminal Procedure)

Two inspections were carried out in 2011 in respect of compliance with Article 8a of Act No. 141/1961 Coll., on criminal court proceedings, and the ensuing compliance with the duties of the personal data controller stipulated by the Personal Data Protection Act in relation to the provision of information to the public and the media on the course of investigation of a natural person; both cases related to the procedure of the Police of the Czech Republic.

The inspection did not prove that the Police of the Czech Republic would disclose to journalists any individual pieces of information that would lead to disclosing the identity of the complainant for the purposes of the news report.

Where information on a specific data subject is collected from several sources within a news report, it is possible that after its broadcasting, the data subject will become identifiable only for a certain specific circle of persons.

Administrative proceedings

(Compliance with Articles 8a to 8c of Act No. 141/1961 Coll., on criminal court proceedings – the Code of Criminal Procedure)

In administrative proceedings, the Office dealt with a case of publication of information that had led to identification of the aggrieved person in criminal proceedings pursued against the

accused person by the Police of the Czech Republic, inter alia, for a misdemeanour of extortion pursuant to Article 175 (1) of Act No. 40/2009 Coll., the Criminal Code, because the accused person had published copies of the resolution of the district state attorney's office and the search warrant issued by the district court, which comprised the name, surname and, in one instance, also the date of birth of the aggrieved person and the name, surname and date of birth of her partner, and also the initial digits of their mobile telephone numbers.

When determining the amount of the penalty, the Office took into account as an attenuating circumstance particularly the fact that the publication was only concerned with a single person (the aggrieved person). The Office also took into account that the relevant articles had low visitor rates.

The Office also took into consideration the nature of the conduct which is considered to be a criminal offence and by which the complainant was harmed. As an aggravating circumstance, it viewed the context of the conduct as follows from the relevant pleadings and documents in the criminal proceedings that were published, because the actual description of this conduct aimed against the aggrieved person can be perceived as infringement of her privacy. After having evaluated all these circumstances, the Office decided to impose a penalty close to the lower limit of the statutory range.

Another decision related to the "Muzzle Act" was an administrative decision concerning the publication of information that a minor person was an aggrieved party in criminal proceedings pursued by the Police of the Czech Republic for the felony of sexual abuse pursuant to Article 187 (1) and (2) of Act No. 40/2009 Coll., the Criminal Code. The information was made public by a party to the proceedings – the publisher of a well-known magazine – in an article published in 2010, where the article included the name and surname of the aggrieved minor. According to the decision of the Office, the publisher of the magazine committed an administrative offence pursuant to Article 45a (1) and (3) of the Personal Data Protection Act, because he breached the prohibition of publication of personal data stipulated by another legal regulation (the Code of Criminal Procedure) and committed this act by printing the given information.

An appeal lodged by the publisher was dismissed by the President of the Office as the appellate body.

The party to the proceedings – the said publishing company – pleaded the absence of a final judgment on guilt in the given proceedings. In his decision on the appeal, the President summarised that the prohibition to publish information on minor persons was not bound to a judgment on guilt. It is sufficient if proceedings are being conducted in respect of a certain act. The President of the Office emphasised that if the opposite interpretation should prevail, this would deny the very meaning of Article 8b (2) of the Code of Criminal Procedure, because the privacy of the minor would be in no way protected until the judgment came into legal force and the protection guaranteed by this provision would lack any sense. The appellate body, i.e. the President of the Office, stated, *inter alia*, that Article 8b of the Code of Criminal Procedure as amended by Act No. 52/2009 Coll. should be construed in that the duty not to disclose information applies throughout the period from initiation of the criminal proceedings to their termination, regardless of the manner of conducting the proceedings. In its conclusions, reached by use of both standard and non-standard interpretation methods, the appellate body also followed, *inter alia*, from the explanatory memorandum to Act No. 52/2009 Coll. (the Chamber of Deputies of the Parliament of the Czech Republic 2006–10,

parliamentary press No. 443), where it is stated, among other things that *"it is necessary to protect the victim (the aggrieved person) in view of his or her age or nature of the case, where detailed information is provided on the identity of the victim, his or her family and privacy, because if this information is published, the victim has to deal not only with the consequences of the crime, but also with the unfavourable impact of the increased public interest in his or her case, which could result in further harm"*. According to the appellate body, i.e. the President of the Office, it is also fundamental not to neglect the fact that any dissemination of information on an identified or identifiable person is an interference with his/her personality, for which the person disseminating such information requires clear statutory authorisation, because it is this authorisation that establishes the duty of the given person to tolerate such interference. The appellate body noted that publication of information to the effect that a minor person is in the position of an aggrieved party in criminal proceedings conducted for suspected felony of sexual abuse would be at variance with Article 8b (2) of the Code of Criminal Procedure, since none of the exemptions pursuant to Article 8b (5) of the Code of Criminal Procedure had been proven as relevant, with the resulting possible waiver of the duty imposed by Article 8b (2) of the said Code. The appellate body considered the amount of the imposed fine to be appropriate in view of the extent of the consequence caused, which is derived from the seriousness of the conduct following from the manner of commitment of the given offence: The information had been disseminated in a magazine and could thus be found at any time in the future; the aggrieved person was very young; and account was also taken of the nature of the criminal offence that was allegedly committed against her; it was also taken into account that, in view of the nature of the matter, the party to the proceedings must have been a professional in the field of journalism and media law, since he was publishing a number of periodicals; moreover, account was taken of the purpose of administrative punishment, which is generally identical with the purpose of punishment in criminal law. The appellate body of the Office therefore decided to dismiss the appeal lodged by the party to the proceedings.

HANDLING OF COMPLAINTS AND CONSULTANCY

For the first time over the six years of existence of the Public Relations Department, the trend of dynamically growing number of instigations and complaints concerned with unlawful conduct in personal data processing stopped last year. The Office received a total of 1,119 instigations and their number thus increased only slightly, by 8 %, compared to 2010. This fact had a positive impact in terms of stabilisation of all the activities pursued by the staff of this department, i.e. the initial legal assessment of the contents of the pleadings in terms of breach of the duties in personal data processing, answering of inquiries and requests for legal interpretation and the provision of personal consultations to data controllers and processers as well as to individuals.

Complaints handled in 2011	
Total	1119
of which:	
referred for inspection	197
referred for initiation of proceedings	70
forwarded to the competent bodies	30
dismissed as unfounded	822

As to the areas of concern of the complaints, the highest number in the long term was related to the operation of video surveillance systems (230 pleadings). A positive development was noted in the approach of the operators of video surveillance systems to the performance of their statutory duties. The residence and workplace of data subjects remain practically the only problematic places monitored by cameras. The future efforts of the Office will be focused on residential buildings, while surveillance at workplaces, which violates primarily the Labour Code, will continue to be resolved in co-operation with labour inspectorates.

The greatest increase in the number of pleadings was recorded in 2011 in the area of modern information technologies, etc., which can be generally denoted as the area of Internet (220 pleadings). In this area, the data subject loses control over the published information, which can then be simply further disseminated and managed in digitalised form.

A topical issue is related to the publication of personal data of natural persons on the Internet by other users, e.g. by the former partner. The Office recorded a marked increase in the number of complaints of this kind. In each case, it is primarily necessary to examine the position of the person who manages personal data without consent of the person with whom the data are concerned. This usually will be a civil dispute and the affected person can naturally request that this information be deleted, or contact the website administrator with this requirement.

Another phenomenon encountered by the Office in 2011, particularly within its consultancy activities, is also related to modern technologies – the use of "clouds". Within the ensuing questions, it must be highlighted that data controller is obliged to comply with Article 13 of the Personal Data Protection Act, which provides for duties in securing personal data. The controller must thus place emphasis on the selection of a credible provider of the storage area or computing capacity, and provide in a contract for organisational and technical parameters of utilisation of the cloud, including the corresponding guarantees of security of the data stored in the cloud. In the event of escape of any information containing personal data, the liability for this situation is borne by the controller. It therefore cannot be recommended to use a cloud in third countries whose legal systems do not guarantee standard protection of personal data.

An extensive homogeneous area was represented by complaints received (115) in respect of the procedure of municipal authorities, where these complaints were most frequently concerned with unauthorised publication of the identity of persons making inquiries pursuant to the Free Access to Information Act and publication of recordings from the meetings of municipal assemblies. In relation to the media coverage of the latter issue, negotiations were initiated with the Mayor of the Capital City of Prague with the aim to find a systemic solution respecting the principles of protection of personal data, which should also be facilitated by co-operation with the authority competent in this area, i.e. the Ministry of Interior.

FINDINGS OBTAINED IN ADMINISTRATIVE PROCEEDINGS

In administrative proceedings conducted by the Office, the latter deals with various aspects related to violation of the Personal Data Protection Act, as well as special laws, particularly the Act on Certain Services of Information Society and Act No. 133/2000 Coll., on registration of the population and birth numbers and on amendment to certain laws (Act on Registration of the Population).

Every year, the Office obtains findings from the administrative proceedings it holds and, by publishing this information in its Annual Report, it contributes to avoiding certain issues in the coming years.

Last year, this was true particularly of **the subject of publication (or in general, disclosure) of personal data of applicants for information** pursuant to Act No. 106/1999 Coll., on free access to information, **and the duty to process accurate personal data** stipulated by Article 5 (1) (c) of the Personal Data Protection Act.

ON THE ASPECTS OF PUBLICATION (OR IN GENERAL, DISCLOSURE) OF PERSONAL DATA OF APPLICANTS FOR INFORMATION

Nothing in the Free Access to Information Act (in any other legal regulation neither) requires or allows the obliged persons to publish personal data of applicants for information. While Article 5 (3) of the said Act requires the obliged entities to publish information provided to the applicant within 15 days of its provision in a manner allowing for remote access, nevertheless this provision clearly does not aim at identifying the individual applicants, but rather at allowing, in public interest, the general public to become acquainted with information provided to the applicant. Indeed, the fact that publication of these personal data is not permissible can also be inferred from Article 8a of the Free Access to Information Act, according to which the obliged entity shall provide personal data only in conformity with the legal regulations providing for protection of these data, i.e. in conformity with the Personal Data Protection Act, which, as noted above, does not permit this procedure.

ON THE DUTY TO PROCESS ACCURATE PERSONAL DATA

It follows from the findings of the Office that the party to proceedings conducted by the Office in relation to distance contracts (call centre) has failed to verify the accuracy of the birth numbers communicated by the clients, even in cases where a certain identical birth number could be found in its records in relation to two persons with different name, surname and address.

Generally, in the opinion of the administrative authority, it can be noted that it is acceptable if the controller does not verify all personal data of his client in concluding a contractual relationship. However, if the client is in delay with a performance under the contractual

relationship (debt) and the data controller in the position of the creditor is forced to proceed with enforcing of his receivable, it is necessary that the data controller enforce this receivable against the actual debtor rather than against a person whose personal data were provided to the controller by someone in connection with execution of the contract, where the data controller in no way verified the accuracy (correctness) of these data. Indeed, in respect of distance contracts, the risk of provision of inaccurate personal data by the client is undoubtedly greater precisely in view of the means of communication chosen; the controller must therefore approach the personal data and their accuracy in view of this risk.

FINDINGS FROM COURT REVIEWS

The Office is party to a number of court disputes. As regards the findings from judicial decision-making in 2011, we could point out two important areas and two important issues. The first is the long-existing issue of **the competences of the Office following from Article 21 of the Personal Data Protection Act**. The second lies in the **question of whether the Personal Data Protection Act also applies to attorneys-at-law in the performance of the legal profession**.

THE ISSUE OF COMPETENCES OF THE OFFICE FOLLOWING FROM ARTICLE 21 OF THE PERSONAL DATA PROTECTION ACT

In its ruling, the Supreme Administrative Court upheld the opinion adopted by the special chamber established pursuant to Act No. 131/2000 Coll., e.g. in case Ref. No. Konf 56/2009, where it stated: *"The Office is now authorised pursuant to Article 29 of the Personal Data Protection Act, inter alia, to perform supervision over compliance with the duties stipulated by the Personal Data Protection Act, accept instigations and complaints concerned with breach of the duties stipulated by the law, discuss infractions and other administrative offences and impose fines. However, it is not authorised to make decisions on the amount of damages ensuing from breach of the duties of the personal data processor and cannot make decisions on compensation for non-proprietary damage. These powers belong to the courts."*

THE QUESTION OF WHETHER THE PERSONAL DATA PROTECTION ACT ALSO APPLIES TO ATTORNEYS-AT-LAW IN THE PERFORMANCE OF THE LEGAL PROFESSION

The Supreme Administrative Court provided an unequivocal answer, inter alia, in case file No. 1 As 13/2011.

The Supreme Administrative Court specifically stated: *"The complainant contends that the Personal Data Protection Act does not apply at all to the activities of attorneys-at-law, because*

the purpose of collection and processing of personal data is specified exclusively by the client and the attorney is obliged to maintain confidentiality.

In this respect, the court notes that such exclusion cannot be inferred directly from the wording of the Personal Data Protection Act. Indeed, the scope of the Act is conceived very broadly and it also applies – along with public authorities – to natural and legal persons who process personal data (Article 3 (1)), of course unless the processing is intended exclusively for personal needs of a natural person or unless occasional gathering of personal data is involved. The Act thus does not exempt attorneys-at-law from its scope, because they are natural persons and they do not process personal data in the pursuit of their profession exclusively for their personal needs. In a number and perhaps even a majority of cases, the activities of attorneys-at-law involve "occasional", rather than systematic, collection of personal data, which is indeed not subject to the cited Act. However, there are also cases where attorneys process personal data systematically; indeed, if they did not do so, they would not sufficiently defend the interests of their clients.

At the same time, it must be noted that it follows from Article 18 (1) (b) of the cited Act that the data controller is not subject to the notification duty in respect of processing required by a special law or if such personal data are required for the enforcement of the rights and duties following from a special law. In agreement with the defendant, the present court considers that this exemption from the notification duty also applies to attorneys-at-law in the discharge of their profession. Indeed, as the nature of the matter clearly implies, an attorney-at-law does not process personal data arbitrarily, but rather precisely with a view to enforcing the rights and duties on behalf of his client and the mentioned notification duty therefore does not apply to him.

The Supreme Administrative Court has thus reached a partial conclusion that, rather than an exemption from the scope of the Personal Data Protection Act as such, only an exemption from this notification duty can be inferred from the legal regulation.

The court considers that the legal regulation is unambiguous in this respect: not even the defence of interests of the client and adhering to his instructions may lead to knowing violation of the legislation. If this were not so, nothing would prevent an attorney-at-law, e.g. from silencing a witness testifying against his client in criminal proceedings".

REGISTRATION

Similar to previous years, the trend of an increasing number of registration notifications continued in 2011. During 2011, the Office received 4421 notifications of processing data pursuant to Article 16 of the Personal Data Protection Act. In addition to assessment of the notifications received, the Office issues decisions on cancelling registration pursuant to Article 17a (2) of the Personal Data Protection Act. A total of 49 instances of processing were thus cancelled during 2011 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. The Office publishes information on cancelled registrations in the Journal.

In connection with the increasing number of notifications of data processing operations, there have also been an increasing number of notified changes and supplements to previously registered instances of processing. The changes were most frequently concerned with addresses, supplementation of the scope of the processed personal data, categories of

data subjects and supplementation of the processing purposes. In some cases, the registered processing is revised on recommendation of the Office within the proceedings on notification of a change in processing. These are often cases where the registration duty no longer applies to the given processing as a result of adoption of new legal rules or their amendment, in view of the exemption stipulated in Article 18 (1) (b) of the Personal Data Protection Act. In that case it is recommended to the controller to cancel the given registration. Where the notice does not contain all the requisites, the controller is requested to supplement the information.

In respect of dealing with the notifications, several cases of processing were recorded this year in relation to monitoring of company vehicles by satellite surveillance equipment (GPS). The data are processed with a view to automatically generating the logbook of trips, to locate the vehicle for the purpose of optimising organisation of work and also for statistical purposes. The controllers often inquire to the Office as to the notification duty pursuant to Article 16 of the Personal Data Protection Act and the possibility of applying an exemption for the notification duty pursuant to Article 18 (1) (b) of the Act. The decision-making must always be based on the purpose of processing. If the objective of processing lay in the protection of the car fleet, economy of operation and compilation of data for the logbook of trips, it could be stated that such processing of personal data is not subject to the notification duty, because it serves for the exercise of the rights and performance of the duties of the employer following from a special law.

Similar to previous years, the most frequent type of notification related to processing via video surveillance systems (36 % of the total number of notifications). To date, a total of 1586 entities processing personal data through video surveillance systems have been entered in the register of personal data processing. A high percentage of notified instances of personal data processing are constantly related to the use of fidelity cards. Another large area of notified instances of processing was related to the operation of internet stores. Notifications are often concerned with processing of data for the purposes of advertising and marketing, real estate activities, consultancy in the area of social sciences and personal development, cultural, leisure, sports and social activities, provision of personal services, organisation of professional courses, training sessions and other educational events, extra-curricular education and training, creation of databases of clients, suppliers, carriers, business partners, etc.

TRANSFER OF PERSONAL DATA ABROAD

Similar to previous years, the most common ground on which authorisation was granted was Article 27 (3) (a) of the Personal Data Protection Act, i.e. transfer of data with consent or on instruction of the data subject. In application of this exemption, it is necessary that the data controller present to the Office a wording of the consent that clearly indicates for which countries of destination the data subject consents to transfer of his data and who will be the recipient. It must also be clear from the wording of the consent that the data subject acknowledges that the countries to which his personal data will be transferred do not ensure an appropriate level of data protection. Furthermore, the consent must clearly indicate to what extent the personal data will be transferred, and for what specific purpose and for what period of time the consent is granted.

Within the numerous consultations, problems were increasingly encountered in respect of submission of the results of processing of personal data for the purposes of clinical studies evaluating the efficiency and safety of newly developed medicines. Clinical studies are performed, *inter alia*, on consenting patients in the Czech Republic, where the results of these studies are submitted to the clients – pharmaceutical corporations – usually in the U.S.A. Provided that the results of clinical studies are transferred to the U.S.A. or some other third country in the form of encoded data without the coding key allowing for assignment of certain data to a specific person, and it is practically excluded that the data could be assigned to a specific person, it could be considered that the thus-encoded data without a coding key cease to be personal data for the recipient in the third country. In other words, such data can be considered as anonymous in the third country. This opinion is based on Opinion No. 4/2007 of the Article 29 Data Protection Working Party on the concept of personal data (WP 136).

Legislative activities

The year 2011 brought about partial modifications in the powers and also an important new competence of the Office, as a law was adopted to amend three laws concerning the area of electronic communications, personal data protection and services of information society. The amendment introduced the following fundamental changes to the processes of personal data protection and, in addition, modified the related competences of the Office.

In conformity with EU law, a new instrument for the protection of personal data and privacy was defined in the Electronic Communications Act. On the providers of services in electronic communications, it explicitly imposed the duty to deal with data breaches.

With a view to ensuring that data breaches are resolved effectively and also in an appropriate way in relation to the affected persons, the Office can now stipulate the format and terms of the data breach notification. In the light of the fact that this is a new regulatory measure with a fundamental impact on the behaviour of operators, which should support the confidence and safety of the subscribers and users of electronic communication services, the Office shall take its further steps based on negotiations with associations of entrepreneurs in the area of electronic communications and with the competent authorities, the Czech Telecommunication Office and the Ministry of Industry and Trade.

From 2012, the Act on Certain Services of Information Society will enable the Office to perform supervision over dissemination of commercial communications pursuant to the Personal Data Protection Act and, in accordance with this Act, employ processes tailor-made for inspection of personal data processing in the area of electronic communications and automated data processing. Up to now, the Office was forced to proceed according to the obsolete State Control Act. The system of supervision over commercial communications and the mechanism of imposing fines for dissemination of unsolicited commercial communications is established in such a manner so as to enable effective punishment of those who disseminate spam and repeated communications. From now on, rather than by repressive means, the Office shall deal with occasional instances of sending unsolicited commercial communications by remedial measures and recommendations, where any potential claims related to liability and indemnification are to be resolved in these cases by the courts. In respect of the said measures, the concept of commercial communication has been defined more clearly; in aggregate, this should facilitate limitation of unsolicited advertising e-mails disseminated on the Internet by domestic entities.

The President of the Office suggested to the Government that it should take due account of the necessary rules for the protection of personal data in the process of drafting the

legislation. Assessment of the impact of legislative measures on the privacy of individuals (Privacy Impact Assessment – PIA) not only contributes to fostering the initiative and reedom of citizens, but also fundamentally guarantees the effective exercise of public administration, because it includes among the basic requisites of the PIA processes due evaluation of the approaches taken to date and assessment of the need for new methods of data processing introduced by the state, which in aggregate leads to more effective management of public resources. This initiative of the Office was subsequently supported by a decision taken by the Deputy Prime Minister.

In respect of the proposal for utilisation of the social card, at first, the Office's instigations were not taken into account at all and were subsequently incorporated only partially. However, ambiguity persisted as to other purposes of using the social card.

In relation to the "anti-corruption" amendment to the Budgetary Rules Act, the Office found that "transparency at any price" introduced by the Act was at variance with the EU law and the relevant case-law. Therefore, after the comments put forth by the Office were not taken into account, the President of the Office turned to the Chamber of Deputies with a letter addressed to the parliamentary reporter responsible for this amendment.

The Office managed to convince the Ministry of Justice – the authority drafting the outline of the Civil Code – about the impropriety of the provision that would consider the silence of citizens entering marked premises recorded by cameras as "automatic" consent to processing of personal data in making the camera recording, instead of the existing, common and fair legal construction that the operation of a video surveillance system must be purposeful and justifiable by clear existing interests in protection of values protected by the law. The proposed wording was later omitted from the Civil Code.

Within the related agenda, the Office presented to the Ministry of Interior a draft legal regulation of making video and audio recordings of municipal assembly meetings, including conditions of their publication on the Internet.

An enormous challenge and the main legislative topic of 2011 in terms of personal data protection, which however was not closed by the end of the year, was the retention of data created or processed in relation to the provision of publicly available electronic communication services or public communication networks. By virtue of its award of 22 March 2011, file No. Pl. ÚS 24/10 related to collection and use of traffic and location data on telecommunication operations, the Constitutional Court repealed certain provisions of Act No. 127/2005 Coll. and entire Decree No. 485/2005 Coll., which implemented the repealed provisions.[1] In this relation, draft partial amendments to several laws were submitted to the intersectoral commentary procedure.

The commentary procedure was closed by the end of 2011. The Office strongly pushed for incorporation of effective and "automatically applicable" guarantees and limitations of risks within the collection and retention of data. It requested, inter alia, mandatory use of other than only generally declared measures to secure data and the most accurate possible specification of the conditions for use of the data. This can be achieved only by a properly revised and elaborated regulation of the competences and individual procedures of the authorised bodies (not only prosecuting bodies, but also in view of other EU regulations as well as those of the Czech National Bank).

[1] http://nalus.usoud.cz

Foreign relations and international co-operation

Representatives of the Office frequently participated in discussions and considerations related to the contemplated reform of the legal framework for personal data protection in the European Union. In this respect, they put forth comments based on the experience gained over the ten years of practice in a wide range of activities in supervision of protection of personal data in the Czech Republic. They expressed their opinions on the existing and newly proposed methods of supervision over personal data processing, e.g. the process of notification, registration and prior checking of processing operations, as well as on the key concepts of protection, such as the definition of the concept of sensitive data and high-risk processing of personal data. In its comments, the Office strived to place special emphasis on dealing with the current trends in data protection, concerning particularly crossborder sharing of data and the related application and law enforcement, and on clearly defining the position of the national supervisory authorities and the mechanism of their co-operation. The Office perceives the absence of uniform rules for crossborder supervision over personal data processing and effective law enforcement on the Internet as a great weakness of supervision over protection of data processed within web applications and in social networks,

particularly if the administrators of the web services are established outside the EU territory.

The end of the first stage of work concerning the revision of Directive 95/46/EC was marked at the very end of 2011 by a proposal for issuing a brand new regulation that would replace this directive, in parallel in the form of a regulation or a new directive; a text was unofficially published that had been drafted and presented for internal discussion and finalisation by the individual departments of the Commission. As to the earlier concept of revision of the Directive – Communication from the Commission of 4 November 2010 COM (2010) 609 (CELEX: 52010DC0609) – New Challenges for the Protection of Personal Data, in co-operation with the affected ministries, the Office drew up the framework position of the Czech Republic, which was taken into cognisance on 20 April 2011 by the Senate Committee on EU Affairs as Senate press No. K 009/08.

The Office also monitored and contributed through individual comments to the work on amendment to the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

The two years of co-operation among the Polish, Hungarian and Czech offices culminated by issuing a popular-instructive publication with the title "Personal Data Protection. Selected Issues. Guide for Entrepreneurs". This event was accompanied by a number of promotional events in Warsaw, Prague and Budapest, mostly in the form of workshops for the professional public. The book found a response in the Council of Europe and it was also presented to WP29 as an advisory body of the European Commission.

In 2011, the Office also continued to be a member of the international consortium for technical assistance to the supervisory authority for data protection in Macedonia. An employee of the Office continued to participate as the main expert on legislative and procedural issues in assistance to the supervisory authority for data protection in Albania.

In three cases, the Office was invited to take part in evaluation of the level of protection of personal data in fulfilling the requirements of the Schengen Convention (evaluation of Liechtenstein, Iceland and summary evaluation of the Nordic countries of Europe – Denmark, Sweden, Finland and Norway).

A representative of the Office was also invited to participate in the conference of the francophone group for personal data protection in Dakar, the first on the African continent, with the task to provide information on the strategy and concept of communication with the public and dissemination of knowledge on personal data protection among the young generation. Within the presentation of the regional projects and international legal instruments, as a Vice-Chairman of the consultation group on Convention 108 (T-PD of the Council of Europe), she provided information on modernisation of Convention 108.

The year 2011 can also be considered fruitful in the area of new technologies in international co-operation and transborder data protection – new technological standard ISO 29100 – A Privacy Framework was completed. In the area of new technologies, which are often ahead of the possibilities following from the applicable laws, the Office effectively utilises its foreign experience and shares its findings with foreign supervisory authorities. In respect of the "smart metering" or "smart grid" technologies, for the first time, the Office was able to reflect in its approach its findings on the innovative strategy of "privacy by design" obtained in co-operation within the International Working Group on Data Protection in Telecommunications (IWGDPT).

Provided that the principles of "privacy by design" are maintained, the variants of smart meters contemplated and tested so far constitute a minor infringement on privacy and they can be considered as acceptable and safe in terms of personal data protection. However, this certainly does not mean that the thus-secured systems contain anonymous data not subject to supervision by the Office. For further development, it will be necessary to provide for safety and confidentiality of the obtained data and it is only up to the energy-production companies which path they will take in the provision of services not only in the Czech Republic, but also throughout Europe, i.e. whether they will already take the necessary in the design or whether they will make complicated modifications of the applications following their launch. In this respect, the Office offers both its positions and professional statements and mediation of foreign experience in the area of personal data protection and securing privacy of clients.

The Office, media and means of communication

In 2011, the Office again held regular press conferences to balance its activities. These con ferences attract to the Office journalists from printed media - dailies and professional press-agency journalists, as well as representatives of the main radio and television stations. The outputs of the press conferences were then regularly presented already during the noon newscast on the day of the press conference. In the three days following the conference, protection of personal data is the subject of 30 to 60 articles, which usually relate to cases concerned with personal data protection that have already been previously covered by the media.

In annexes to press releases, the Office regularly provides information on controls closed by initiation of administrative proceedings. In this respect, it is important not only that the Office openly discusses the results of its work, but also that it provides a report on the reasons for the imposed fines, whereby it simultaneously raises legal awareness in respect of the Personal Data Protection Act and the manner of its application.

CONTACT WITH THE MEDIA

Based on the daily service for the media, it can be concluded that the aspects of personal data protection are a frequent media topic. However, it must also be noted that the interest of journalists in information leads them in some cases to adopt a position where they prefer access to information without paying much attention to the need for balanced application of all the legal rules and statutory provisions. In 2011, this was manifested particularly in relation to the publication of salaries of government officials and officials of local governments.

Similar conclusions can also be drawn from the focus of direct presentations in the media that are requested from the President of the Office, relevant experts, or the spokeswoman.

The Office usually publishes all the media releases on its website (naturally with agreement of the given media). It thus gives the general public the opportunity to follow the opinions of the Office and provides the journalists with an immediate response to their inquiries.

The “News” section on the homepage of the website serves as a source of readily accessible informatoin on the activities of the Office and its current agenda.

DISSEMINATION OF KNOWLEDGE ON PERSONAL DATA PROTECTION

The Personal Data Protection Day in January always offers an opportunity, not only to provide information on the everyday agenda of the Office in the past period, but also to discuss personal data protection in more general terms in the context of the right to privacy as a fundamental human right.

In 2011, the Office announced the fifth edition of the competition for children and youth in the Czech Republic entitled ""This is my privacy! Don't look, don't poke about!". In its activities focused on the young generation, the Office has traditionally co-operated with the Czech Radio Prague, the International Festival of Films for Children and Youth in Zlín and newly also with the Association of Library and Information Professionals (SKIP). In more than 100 libraries throughout the Czech Republic, children from 7 to 10 years of age competed in the Through the Wild Web Woods game, which teaches them in an entertaining way how to behave safely and respectfully on the Internet. The Office co-operated in the preparation of the Czech version of the game with the Council of Europe, which had prepared this entertaining form of training of safe behaviour in the environment of the Internet.

The Office was largely involved in various conferences and workshops. In co-operation with the F.S.C. company, the Office organised two conferences on data security. A workshop organised by Wolters Kluwer Czech Republic with participation of the President of the Office and an employee of the registration department was dedicated to the subject of use of video surveillance systems in schools. Moreover, 40 events were held and employees of the Office provided lectures on personal data protection for 31 academic, legal, business and public-law institutions.

LIBRARY AND PUBLICATIONS OF THE OFFICE

The library continues to serve as a source of professional information for employees of the Office, but is also open on individual request to professional public.

In 2011 the Office published the 60th volume of its Official Journal. Two special issues of the Information Bulletin were dedicated to processing of genetic data related to the use of DNA samples and the legislative issues connected with the topic of video surveillance systems and the associated legislative problems. The issue concerned with the use of cameras raised particular attention of the media.

WEBSITE OF THE OFFICE

The scope of information provided on the website is usually positively accepted by professional and general public in terms of contents. In view of the fact that a relatively long period of time has already elapsed from the time when the website was created, the Office resolved to innovate the website in terms of its technical modernisation, which also allows for faster search in the contents which are not quite extensive.

ORG Information System

The year 2011 was marked by the development of the "ORG Information System" project. 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 with a system of meaningless identifiers. These identifiers will differ for the individual agendas or groups of agendas and will thus not allow to 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 does not contain any names of natural persons and, therefore, even knowledge of all identifiers does 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 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 – Convergence Goal, area of support Development of Information Society in Public Administration. The Structural Funds Department of the Ministry of the Interior of the Czech Republic approved the said project on 30 November 2009.

Personnel of the Office

102 functional positions were stipulated for the Office by the 2011 State budget.
As of 1 January 2011, the Office had 101 employees, of which 96 were in the records and 5 outside the records.
As of 31 December 2011, the Office had 104 employees, of which 99 were in the records and 5 outside the records.
Eight new employees were hired by the Office and six employees ceased working for the Office during the year.

Classification of employees of the Office according to education and sex – as of 31 December 2011

Education	men	women	total	%
Secondary vocational + vocational certificate	1	1	2	2.0 %
Secondary vocational	0	1	1	1.0 %
Full secondary general	3	5	8	8.1 %
Full secondary vocational + vocational certificate	1	1	2	2.0 %
Full secondary vocational	4	16	20	20 %
Secondary vocational education	0	2	2	2.0 %
University	39	23	62	62.6 %
University + higher qualifications	1	1	2	2.0 %
Total	49	50	99	100.0 %

Economic management of the Office

The budget of the Office was approved by Act No. 433/2010 Coll., on the State budget of the Czech Republic for 2011.

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

	in CZK thousand
Summary indicators	
Total income	63 888.70
Total expenditures	166 689.66
Specific indicators – income	
Total non-tax and capital income and accepted transfers	63 888.70
of which: total income from the budget of the European Union. excl. SZP	63 482.65
other non-tax and capital income and accepted transfers, in total	406.05
Specific indicators – expenditures	
Expenditures to ensure performance of the tasks of the Office for Personal Data Protection	166 689.66
Cross-cutting expenditure indicators	
Salaries of employees and other payments for performed work	44 211.59
Mandatory insurance premiums paid by the employer*)	15 609.10
Contribution to the Cultural and Social Needs Fund	424.46
Salaries of employees within an employment relationship	34 289.54
Salaries of employees derived from salaries of constitutional officials	8 165.00
Total expenditures co-financed from the budget of the European Union. excl. SZP	
of which: from the state budget	11 488.02
contribution from the EU budget	65 375.08
Total expenditures recorded in the information system of programme financing	82 454.37

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

Provision of information pursuant to act No. 106/1999 coll., on free access to information, as amended

In 2011, the Office received a total of twenty-three requests for information pursuant to the Free Access to Information Act. By comparison with the previous years, it can be stated that the number of requests for information is constantly increasing.

Of the total number of requests for information in 2011, the Office fully satisfied seventeen requests, partially dismissed four requests, where it provided limited information, and dismissed the request for information as a whole in two cases. 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 Free Access to Information Act.

Similar to the previous year, the applicants most often requested that they be sent specific administrative acts or other official documents of the Office, other documents of the Office, e.g. the inspection plan for 2011, information on the results of proceedings held by the Office, etc.

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

Annual Report Summary 2011
The Office for Personal Data Protection
Pplk. Sochora 27, 170 00 Praha 7
E-mail: posta@uoou.cz
Web: www.uoou.cz

In February 2012, 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