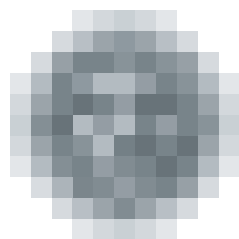


ANNUAL REPORT SUMMARY

2012



**úřad pro ochranu
osobních údajů**

the office for personal
data protection

The President of the Office looks back at 2012



The past year must be viewed as a year of new trends and technologies. The Office for Personal Data Protection must still confront reality, which means, on the one hand, increased user comfort through miniaturised technology and interconnection of various systems and, on the other hand, an increased number of central data storages, which are highly vulnerable to attack, particularly against sensitive data.

The Office entered the year 2012 with a new area of competence in “data breaches” – i.e. in the field of personal data processing in electronic communications – where the Office is newly obliged to monitor the situation and check the effectiveness of solutions adopted by entrepreneurs providing a publicly accessible electronic communications service; such an entrepreneur, if he detects breach of security of personal, traffic and location data and confidentiality of communication, must notify the Office without undue delay.

Another challenge for the Office lies in the new legal framework of personal data protection in the EU, where a number of new trends, such as “privacy by design” and “privacy impact assessment” have already become part of the future legal regulation of the conditions of personal data protection, rather than a mere proclamation of these principles by the obliged persons on the internet. Although the discussions on the legal framework within the European Commission have been relatively protracted to date, it is already possible to predict where the future supervision competences of the Office should lie. I appreciate that the Czech Government is not lagging behind in this respect. I also firmly believe that a new duty introduced by the Government will be systematically adhered to starting next year, specifically

that the impact on privacy will be evaluated by the time that each new legal regulation is submitted. This will prevent situations where the possible drawbacks related to personal data protection are ascertained only after the given laws and regulations have already been adopted.

When mentioning new notions and trends in the development of services in the information society, I must also consider the topical issue of development and use of “cloud computing”, which has literally been on the table every day. The Czech Republic is certainly no exception in this respect and will have to deal with this subject. We therefore appreciated when, in July 2012, the Working Party for Data Protection established pursuant to Article 29 of Directive 95/46/EC (Article 29 Working Party) issued its opinion 05/2012 dealing with “cloud computing”. The document indicates how closely the aspects of personal data protection are connected with the development and application of the latest technologies and how urgent it is to take into consideration, already at the stage of designing new services, both the role of the “cloud computing” service provider and the position of the users of this new service from the viewpoint of responsibilities of the individual stakeholders pursuant to the Personal Data Protection Act.

The fact that we are not ignorant of these trends is also reflected in a number of meetings and presentations by representatives of the Office at conferences concerned with new technologies and personal data protection in relation to their development. New trends in the use of surveillance systems and cameras, such as photo traps and other deployment of surveillance technology – the use of cameras in cars to monitor road traffic or the development of “smart” housing – have also brought new challenges for the Office, which has to deal with the situation, not only in terms of the actual application of the Personal Data Protection Act, but also in considering the potential impact on the privacy of the monitored persons.

I am glad that many citizens and organisations turn to the Office and point out the shortcomings of modern times, where it is very easy to interfere with the formerly entirely private spheres of each of us. While the Office is not empowered with absolute supervision in the area of protection of privacy, it strives to create an environment in the field of personal data processing so as to promote those trends that will guarantee and strengthen the right of individuals to protection against unauthorised processing of their personal data.



Igor Němec

Table of Contents

OFFICE IN NUMBERS – 2012	8
CONTROL ACTIVITIES OF THE OFFICE	10
■ 2012 CONTROL PLAN	10
I. General topics for specification of control activities of inspectors of the Office	10
1. Public administration information systems	10
2. Information systems in the area of private law	11
3. Processing and disclosure of personal data in the area of crime prevention and fight against terrorism	12
II. Inspections from the 2011 control plan, completed in 2012	12
Inspection of CSO – census of the population, buildings and apartments in 2011	12
Inspection of private entities operating a business in the area of social care	12
Inspection concerned with personal data processing in relation to the use of passive identification bracelets for patients	13
Control of customer cards	13
Control of customer data in Alza.cz	13
Control of compliance with the rules for disclosure of data in telephony	13
III. Inspections initiated in 2012 on the basis of an instigation of the President	14
Inspection of the Superior State Attorney’s Office in Prague	14
Inspection of Czech Post	14
Inspection of the Prison Service of the Czech Republic	14
IV. Inspections initiated in 2011 on the basis of an instigation of the President and completed in 2012	14
Inspection of the Central Bohemian Region – provision of a special-purpose gift for payment of regulatory fees	14
Inspection of the Municipal Court in Prague – processing of complainants’ personal data	15
■ FINDINGS OBTAINED BY INSPECTORS IN CONTROL ACTIVITIES	16
Database of DNA profiles	16
Right to information while respecting the right to personal data protection	17

Debtors' personal data published on the website of an Association of Residential Unit Owners	17
Internet competitions for children	18
Health care	18
Inspection concerned with personal data processing through customer cards – Česká lékárna, a.s. (network of Dr. Max pharmacies)	18
Inspection concerned with the submission of data on patients within screening of oncology diseases	19
Control of keeping medical records in a health-care facility	20
Instigation against the General Health Insurance Company of the Czech Republic	21
Inspection concerned with personal data processing in relation to the use of passive identification bracelets for patients – Na Homolce hospital	21
Camera surveillance systems	22
Superior State Attorney's Office in Prague	22
Camera surveillance system on business premises	23
Camera surveillance system in a social care facility	24
Municipal camera surveillance system	25
Prague Airport – inspection concerned with personal data processing with the use of records from camera surveillance systems installed in publicly accessible areas of the airport	25
Camera surveillance systems in an apartment building	27
Management of sensitive personal data of clients of a retirement home and processing of their personal data through a camera surveillance system with cameras installed in the rooms and common premises	28
■ ADDRESSING COMPLAINTS AND PROVISION OF CONSULTATIONS	29
■ FINDINGS OBTAINED IN ADMINISTRATIVE PROCEEDINGS	31
“False” contracts	31
Publication of information (photographs or parts or recordings) obtained with the use of a camera surveillance system with a view to detecting offenders	33
■ FINDINGS FROM COURT REVIEW	34
Tax administration	34
Performance of supervision by the Office	34
Failure of the data subject to express disagreement with personal data processing cannot be considered consent pursuant to Article 4 (n) of the Personal Data Protection Act	34
Unsolicited commercial communications	35

Extensive and undifferentiated use of a camera surveillance system is at variance with Article 5 (2) (e), the part of the sentence after the semicolon, of the Personal Data Protection Act, which requires that the right of the persons being recorded to protection of privacy and personal life be maintained	35
■ REGISTRATION	35
■ TRANSFER OF PERSONAL DATA ABROAD	38
LEGISLATIVE ACTIVITIES	40
RELATIONS TO FOREIGN COUNTRIES AND INTERNATIONAL CO-OPERATION	42
THE OFFICE, MEDIA AND MEANS OF COMMUNICATION	45
ORG INFORMATION SYSTEM	47
PROJECT OF "OPTIMISATION OF PROCESSES OF THE OFFICE"	48
PERSONNEL OF THE OFFICE	49
ECONOMIC MANAGEMENT OF THE OFFICE	50
PROVISION OF INFORMATION PURSUANT TO ACT NO. 106/1999 COLL., ON FREE ACCESS TO INFORMATION	52

Office in numbers

2012

Inquiries and consultations	inquiries in the Czech Republic	2503
	abroad	47
	consultations	2358
	for state administration	139
	for local governments	190
	for legal persons	307
	for natural persons operating a business	257
	for natural persons	1548
Pleadings and complaints	instigations received pursuant to the Personal Data Protection Act	1319
	complaints referred for inspection	197
Unsolicited commercial communications (competence pursuant to Act No. 480/2004 Coll.)	total instigations	7933
	instigations resolved	3772
	inspections initiated	87
	inspections completed	88
	administrative decisions on a fine	23
Inspections (excluding inspections concerning Act No. 480/2004 Coll.)	initiated	129
	completed	138
	referred to other governmental authorities	2
	challenged by objections	16
	objections accepted	3
	objections dismissed	7
	mostly accepted	0
	mostly dismissed	5
Administrative punishment	administrative proceedings for violation of Acts No. 101/2000 Coll. and No. 133/2000 Coll.	118
	infraction proceedings pursuant to Act No. 101/2000 Coll.	21
	administrative and infraction proceedings pursuant to Act No. 101/2000 Coll. - Articles 44a and 45a	3
	infraction proceedings for violation of Act No. 159/2006 Coll., on conflict of interests	0
	appealed decisions on violation of law	43
	appeals dismissed	31
	cancelled and returned for new hearing	4

	cancelled decisions and proceedings discontinued	8
	change in the decision	9
Judicial review (NB: * in total since 2001)	court actions lodged	9 (100*)
	actions dismissed by the court	5
	decisions cancelled by the court	3
	court proceedings closed / pending since 2001	59/41
Registration	notifications received (pursuant to Article 16 of Act No. 101/2000 Coll.)	5169
	instances of processing registered	4618
	still pending	969
	registrations cancelled	78
	notifications on a change in the processing	811
	proceedings pursuant to Article 17 discontinued (no violation)	108
	discontinued for procedural reasons (e.g. notifications withdrawn)	100
	not permitted	6
		2
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.)	18
	decisions on authorisation of transfers	13
	decisions on dismissal	0
	proceedings discontinued for procedural reasons	5
Notifications pursuant to Act No. 127/2005 Coll.	notifications received	2
	notifications found justified	1
	notifications found unjustified	1
Complaints pursuant to Article 175 of the Code of Administrative Procedure	complaints received	26
	complaints found justified	5
	complaints found partly justified	5
	complaints found unjustified	16
Applications pursuant to Act No. 106/1999 Coll.	applications received	42
	fully accepted	29
	partly accepted	10
	applications rejected	3
Materials published	Official Journal (number of volumes)	3
	Information Bulletin (number of volumes)	1
Press conferences	regular	2
	extraordinary	0
Legislative drafts on which comments were made	laws	85
	implementing regulations	94
	draft government regulations	14
	draft decrees	80
	other	55
	foreign materials	76

Control activities of the Office

■ 2012 CONTROL PLAN

I. GENERAL TOPICS FOR SPECIFICATION OF CONTROL ACTIVITIES OF INSPECTORS OF THE OFFICE

1. PUBLIC ADMINISTRATION INFORMATION SYSTEMS

Personal data processing by governmental authorities is one of the areas that are regularly monitored by the Office.

The Office therefore carried out control of protection of citizens' personal data in application of the provisions of Act No. 106/1999 Coll., on free access to information, as amended, by cities and towns. Within this item of the plan, the appointed inspector performed two inspections in statutory cities.

In conformity with the commitments of the Czech Republic in the area of EU's 3rd pillar, including the Schengen Convention, and further to the results of evaluation of compliance with these commitments, which was carried out in February 2012, the Office performed a regular inspection of the Police of the Czech Republic as required by the National Schengen Plan for 2011.

The inspection was concerned with the area of entering personal data pursuant to Article 96 of the Schengen Convention and the procedure in dealing with applications of data subjects for access to personal data, exercise of their right to rectification/deletion of personal data processed in the SIS (Art. 109 and 110 of the Convention), security measures in ensuring access of authorised entities to the data stored in the SIS and in subsequent management thereof, including the scope, procedure and effectiveness of internal control by the Police of the Czech Republic (control of logs as required by Art. 101 of the Convention).

Based on the inspection, the Office noted violation of Article 13 (1), (2) and (3) of the Personal Data Protection Act on the grounds of failure to adopt adequate measures to prevent unauthorised access to personal data in the Schengen Information System where, at the time of the inspection, the responsible entity did not record specific reasons for making searches in the SIS pursuant to Article 63 of the Act on the Police of the Czech Republic, although a police officer is authorised to request proof of identity of a person sought by the police only on the grounds set out in the said provision.

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:

- **the conditions of personal data processing in relation to offering and acceptance of services**, which may include issuing of loyalty customer cards in all types of services; the Office focused on compliance with the duties of the responsible persons in gathering this information directly from the individual entities and their further legitimate disclosure to recipients;
- **processing and transfer of personal data of passengers; an inspection of České aerolinie, a.s.** took place from 25 April to 16 October 2012 and did not ascertain any violation of the Personal Data Protection Act;
- **processing of customers' personal data in relation to offers of sale of goods and services** (operation of a camera surveillance system, customer cards). Several inspections were initiated within the performance of this task in 2012;
- **processing of personal data of passengers in the operation of camera surveillance systems in means of public transport** The inspection was concerned with compliance with the duties stipulated by the Personal Data Protection Act with special focus on protection of personal data processed using the Municipal Camera Surveillance System of the Capital City of Prague. The city had specified the objectives (purpose) and means of personal data processing – maintaining public policy, protection of the health of citizens and visitors, protection of property and traffic safety. It was found within the inspection that the personal data and recordings from the camera surveillance system collected in public areas of the city within the ascertained scope substantially contributed to the achievement of the set objectives. Processing of the recordings beyond the scope of the set objectives was not ascertained in the inspection;
- **the conditions of personal data processing in negotiations on lease contracts and other related arrangements in the area of housing** The result of the inspection was a recommendation to separate data required for negotiations on lease and user contracts from data necessary for the conclusion and performance of lease and user relationships. In conformity with its plan, the Office performed control of protection of citizens' personal data in administration of the agenda related to lease of apartments owned by cities and towns;
- **the conditions of processing the personal data of customers in offering goods and services**, not only within the Personal Data Protection Act, but also in other areas of competence of the Office in respect of certain services of the information society in the sense of the Act on Certain Services of the Information Society;
- **personal data processing in relation to offering goods and services in the area of electronic communications**. Where shortcomings were found in the inspections,

consisting in the provision of inadequate information to the customers, or non-compliance with the duties related to marketing, the controlled entities were reprimanded and penalised for these breaches.

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

In this area, which is already a traditional part of the supervisory activities of the Office, the inspectors focused on control of performance of the duties of the Czech Republic in relation to the submission and processing of information in the SIS and VIS. For several years, the Office has therefore performed controls of the performance of controllers' duties in personal data protection within the process of granting visas to persons from countries outside the Schengen area.

As previously in Macedonia, Ukraine and Mexico, this time the inspections were again carried out at the embassies of non-Member States of the EU (Kazakhstan, Turkey, Russia) focusing on access to the SIS and safeguarding the applicants' personal data.

II. INSPECTIONS FROM THE 2011 CONTROL PLAN, COMPLETED IN 2012

Inspection of CSO – census of the population, buildings and apartments in 2011

As regards organisational and security measures, the inspectors criticised only the fact that the envelopes with the filled-in form could be sent by putting them directly in the post box, in which case it was not possible to verify whether the forms with personal data were indeed properly delivered to the Czech Statistical Office. Nonetheless, save for the above, the organisational and security measures were in conformity with the legal regulations and the criticism outlined above also does not involve any demonstrated violation of Article 13 of the Personal Data Protection Act.

The forms have yet to be submitted to the National Archive and it is thus not possible to establish conformity or non-conformity with the law in this respect; however, within the inspection, the inspectors suggested changes to the relevant procedures so as to ensure anonymisation. The Czech Statistical Office agrees with the suggestions made by the inspectors.

As to statistical data that will be further processed after the census is completed, the CSO was also advised by the inspectors of the principles that must be adhered to, which means that no personal data originating from the 2011 census may be processed after expiry of a period of three years.

Inspection of private entities operating a business in the area of social care

Inspections were carried out in three limited liability companies. Two of these inspections were carried out in collaboration with the Office of the Public Defender of Rights (the Ombudsman) and revealed violations of the Personal Data Protection Act, mainly in the use of camera surveillance systems with recording equipment, where the conditions for processing of this information were not fully respected in view of the privacy of the monitored persons.

Inspection concerned with personal data processing in relation to the use of passive identification bracelets for patients

The inspection revealed no breach of duties of the personal data controller in processing personal data.

Control of customer cards

An inspection in this area was concerned with personal data processing through customer cards – Česká lékárna, a.s. (network of Dr. Max pharmacies) The inspector concluded that the processing occurred on the basis of consent of the consumers – data subjects in conformity with information properly provided to them.

Control of customer data in Alza.cz

The inspection was concerned, on the one hand, with safeguarding the personal data of the customers and other persons in relation to the business activities with the use of an information system and, on the other hand, with compliance with the conditions stipulated for dissemination of commercial communications.

The inspection revealed the fact, which is by no means rare in the Office's practice, that the users of e-mail addresses or telephone numbers often provide their data in relation to the purchase of goods or register themselves on the website of the service provider. The controlled entity unambiguously proved that all the e-mail addresses and telephone numbers were obtained in relation to the sale of its products or services. Consequently, prior consent was not required in relation to sending commercial communications and the customers' data were used on the basis of their purchase of goods.

It was noted within the inspection that, unlike in e-mail communication, the customers using sms services were not provided with a clear and distinct opportunity to refuse consent to such a use of their electronic contact details in a simple manner and free of charge or at the expense of the sender. In this relation, the inspection highlighted the issue of compliance with the said duty, particularly in respect of commercial communications sent by sms messages. The senders of commercial communications usually perform their duty by providing information in their general terms and conditions, but fail to do so within each individual communication. The inspector of the Office thus recommended to the controlled entity in which way it should modify the wording of the sms messages so that the latter contained information on the manner in which the recipient could refuse consent to sending sms messages containing commercial communications in a simple way, free of charge or at the expense of the sender. At the same time, the inspection did not prove that the controlled entity would have violated the Personal Data Protection Act in processing of personal data of customers and other persons in relation to its business activities.

Control of compliance with the rules for disclosure of data in telephony

Based on its plan, the Office followed up on an instigation against Telefónica O2, which proved by the relevant documents that an external salesperson had used one e-mail address for several subscribers. In April 2012 the competent manager of Telefónica O2 ascertained this breach, the incorrect e-mail address was removed from the database of subscribers and the salesperson was penalised. In view of the findings set out above and in conformity with Article 29 (1) (c) of the Personal Data Protection Act, the ascertained violation of the Act was the subject of administrative proceedings pursued by the Office. The proceedings were closed by imposing a fine.

III. INSPECTIONS INITIATED IN 2012 ON THE BASIS OF AN INSTIGATION OF THE PRESIDENT

Inspection of the Superior State Attorney's Office in Prague was initiated based on published information (recording from a camera surveillance system) and in view of a public instigation, and the President of the Office decided that inspection would be carried out in the Superior State Attorney's Office in Prague in respect of camera recordings made at the seat of the controlled party, on the grounds of a justified suspicion that the procedure of the persons responsible for the operation of the system and disclosure of information – personal data of the monitored persons – constituted breach of the controller's (or processor's) duties pursuant to the Personal Data Protection Act.

Inspection of Czech Post followed up on an instigation to initiate administrative proceedings related to monitoring of employees of Czech Post, and was a response to information published in the media on monitoring of employees of Czech Post by means of the GPS technology and their localisation, which apparently involved unlawful processing of the employees' personal data obtained from the personal terminals of the postmen. The inspection was also initiated in view of the fact that in 2010 and 2011 the Office had provided Czech Post with consultations and gave it certain recommendations, with which the practices in question were in clear contradiction.

The inspectors noted violation of the Personal Data Protection Act, because they found no legal grounds for consistent processing of personal data and monitoring of the whereabouts of the postmen throughout the district in which they performed their profession. Czech Post raised objections against the finding; the objections are subject to assessment by the President of the Office.

Inspection of the Prison Service of the Czech Republic in relation to publication of photographs of persons remanded in custody. It was clear from publicly accessible sources that photographs of persons remanded in custody were published on 2 and 5 June 2012, where the images had originally been taken for the purposes of remand and the related processing of personal data.

The inspection revealed violation of the Personal Data Protection Act, as personal data had leaked from the Prison Information System. On the basis of intervention by the inspector performing the control, a fundamental change was made in the access rights of the employees of the Prison Service. Currently, only those employees of the Prison Service of the Czech Republic who need the data for the performance of their duties have access to the personal data of persons in custody located in a different prison.

IV. INSPECTIONS INITIATED IN 2011 ON THE BASIS OF AN INSTIGATION OF THE PRESIDENT AND COMPLETED IN 2012

Inspection of the Central Bohemian Region – provision of a special-purpose gift for payment of regulatory fees

The inspection revealed violation of the Personal Data Protection Act in that the Central Bohemian Region published on the website lists of personal data of those persons who had been provided with a gift for payment of regulatory fees in health care, or who, to

the contrary, had refused the gift. The Central Bohemian Region thus enabled unauthorised access to the personal data by third parties. The President of the Office rejected the objections raised by the Central Bohemian Region and the Office made a decision on administrative punishment and imposed a fine.

In the proceedings, the Office noted that the procedure of the Council of the Central Bohemian Region in the given case must be assessed in terms of proportionality between the right to information and the right to protection of privacy.

In publication of certain information, it is generally necessary to distinguish two situations – on the one hand, publication of information intended for authorised persons (i.e. the applicant in the given case) and, on the other hand, publication on a website, where the information, including personal data, is disclosed to an unlimited scope of recipients.

At the same time, publication of personal data in a manner allowing for remote access (via the Internet) for a previously unspecified group of persons based on the personal initiative of the obliged entity clearly interferes with the personal sphere of an individual much more than disclosure of the data based on an individual application by a specific natural or legal person.

Based on the proportionality test, limitation of fundamental rights and freedoms is possible only if the interference is suitable, necessary and appropriate for attaining the set objective.

Those who refused the gift were clearly not recipients of public funds at the given time and there was thus no legal reason for publishing their personal data. In respect of those who lodged the application (for a gift), the Office then considered that the Central Bohemian Region could have fulfilled its duty to provide information on public expenditures by providing, on its website, information on the total number of recipients to whom the gift was provided and on the total amount of the funds thus expended, on the structure of these public funds, etc.

The aforesaid considerations thus lead to an unambiguous conclusion that the right of access to information is also not unlimited; even if the conduct of the Central Bohemian Region could be considered as having legal grounds in increased transparency and public control of the public expenditures, publication of personal data on the internet within the scope set out in the operative part of the decision cannot be deemed appropriate or necessary as it constitutes inappropriate interference with the right to protection of private and personal life.

Inspection of the Municipal Court in Prague – processing of complainants' personal data

The Office received a complaint related to a justified suspicion that the Court had been unlawfully, and without justification, collecting information and data on the complainant and subsequently disseminating this information and data, where the judge refused, by his resolution, to allow the complainant to inspect the file. The complainant considered that the Court was processing his personal data at variance with protection of his private and personal life and also at variance with the Personal Data Protection Act, because the personal data were inaccurate and were further disseminated to police corps, the intelligence service and other entities, and requested the Office to investigate the matter, including a request for the relevant files from the Court.

The inspection proved that the Court had not only adopted the necessary measures in the sense of Article 13 of the Personal Data Protection Act, but had also provided for

performance of the relevant duties (specifically in the employees' employment contracts).

Beyond the scope of the said legal conclusion, it was noted that the misconduct in question had occurred in November 2008 and any potential liability of a legal person for the given administrative offence had already expired. Within the inspection, the Court performed further measures beyond the scope of its duties pursuant to the internal office rules.

Breach of the legal duty by the natural person (employee) did not correspond to the merits of an infraction.

■ FINDINGS OBTAINED BY INSPECTORS IN INSPECTION ACTIVITIES

DATABASE OF DNA PROFILES

An inspection of the National DNA Database (hereinafter NDD) was carried out in 2008; the Police of the Czech Republic were required to proceed pursuant to Article 42e (3) of the Police Act: Sensitive personal data may be processed only if ***this is required in view of the nature of the criminal offence for the performance of the tasks of the Police in relation to the criminal proceedings***; as a result of the inspection, the Police were ordered to destroy all the DNA profiles in respect of those offenders who did not meet the said criteria. The Police failed to comply with this remedial measure and, to the contrary, contested the fine by an action lodged with the administrative court.

Based on a number of complaints and in view of the new Police Act, a new inspection was initiated in the middle of 2011; the inspection was closed in September 2012.

Pursuant to Article 9 of the Personal Data Protection Act, sensitive data, including DNA profiles, may be processed only with consent of the data subject or if the data are ***processed pursuant to special laws within prevention, search for and detection of crime, prosecution of criminal offences and search for persons***.

Extensive use of buccal swabs in respect of accused persons where this is not necessary for proving his/her guilt or innocence or for any other investigation of the given criminal offence, for the purposes of future identification, i.e. for investigation of crimes that might be committed in the future, therefore does not pass the test of necessity of such processing in the sense of Article 79 of the Police Act or the constitutional principles of lawfulness and proportionality.

In the inspection protocol, the inspector therefore noted violation of Article 9 of the Personal Data Protection Act and requested destruction of the DNA profiles in the NDD, which was also confirmed by the appellate body, i.e. the President of the Office. A fine has yet to be imposed.

RIGHT TO INFORMATION WHILE RESPECTING THE RIGHT TO PERSONAL DATA PROTECTION

With increasing frequency, municipalities are requested by their citizens and members of municipal assemblies for information on the activities of the municipal bodies, on future plans and on decisions that the municipalities have made within their decision-making powers. Applications for copies of contract and requests for disclosure of the amounts of remuneration of members of the statutory bodies or the salaries of the authority's employees are typical examples.

The control plan and certain *ad hoc* inspections in 2012 focused on whether, in practice, these applications and requests are dealt with in conformity with the law, as it is sometimes difficult to determine whether or not the provision of information is prevented by a legal barrier (e.g. protection of personal data) or business secrets, as well as whether the municipality has this information or is obliged to provide it.

In view of a number of justified complaints that were subsequently dealt with in administrative proceedings, the Office turned directly to the Ministry of Justice of the Czech Republic with a notice of the need for compliance with the law in relation to publication of the personal data of the applicants.

In 2012 this involved thirteen administrative proceedings concerned with unauthorised publication of personal data in relation to the provision of information pursuant to Act No. 106/1999 Coll.

Based on findings from the control activities, administrative proceedings and its consultancy activities and answers to inquiries, the Office states that the Personal Data Protection Act is not being seriously violated within the performance of duties imposed on the obliged entities by the Free Access to Information Act.

DEBTORS' PERSONAL DATA PUBLISHED ON THE WEBSITE OF AN ASSOCIATION OF RESIDENTIAL UNIT OWNERS

An inspection performed in respect of personal data processing by an Association of Residential Unit Owners by means of publication of the personal data of its debtors – members of the Association – on the website of the controlled entity revealed that it was possible to obtain information on six debtors, within the scope of their name, surname and amount of their debt, from the published minutes of the meetings of the committee.

The Association does not require the consent of the debtors to keeping records of debts and of negotiations on the manner of collecting these debts, because this falls within the scope of an exemption pursuant to the Personal Data Protection Act according to which it is possible to process personal data if this is required for the protection of the rights and legally protected interests of the controller, recipient or some other affected person; however, this personal data processing may not be at variance with the right of the data subject to the protection of his or her private or personal life.

As far as personal data processing by means of publication of the debtors' names with the amounts of their debts on the Association's website is concerned, this is not covered by the exemption because the published personal data may be accessed not only by creditors of the debtors, but also by a number of other persons visiting the website. Such an extensive interference with privacy is then usually in disproportion with the possible effects following from improved payment morale of the debtors.

The controlled entity – the Association of Residential Unit Owners – remedied the unlawful state of affairs by protecting the website containing the debtors’ personal data by a password, with secured access only for members of the committee, and no remedial measures were thus imposed. However, a fine was imposed on the controlled entity in spite of the fact that the defective state of affairs was already remedied during the inspection.

INTERNET COMPETITIONS FOR CHILDREN

Based on instigations, the Office carried out several inspections concerned with internet competitions involving children. The following conclusions were drawn within the inspections:

In Article 8, the Civil Code stipulates: *The capacity of a natural person to acquire rights and assume obligations by his/her own legal acts (legal capacity) arises to the full extent upon reaching legal age.* In Article 9, it further specifies: *Minors have capacity only to those legal acts that are, in their nature, appropriate to the intellectual and volitional maturity corresponding to their age.* To the contrary, the parents are *responsible for the emotional, intellectual and moral development of a minor child* (cf. Article 31 of the Family Act and Articles 217 and 217a of the Criminal Code).

The capacity to enter into a “competition contract” and give consent to processing of personal data in competitions of this type will probably often be absent in children under 15 years of age; execution of the said contract will thus require the consent of the legal representative, because these children cannot assess all the impacts of such a contract and consent to personal data processing. The inspectors used, as the decisive criterion, the age of 15 years, because from this age children could be aware, in view of the current information era, that their data will be processed to a certain extent and that, if their personal data are managed at variance with the law, they can claim their rights (albeit only through their legal representatives).

Everyone who organises such a competition must register with the Office for Personal Data Protection, because in any case this involves personal data processing.

HEALTH CARE

INSPECTION CONCERNED WITH PERSONAL DATA PROCESSING THROUGH CUSTOMER CARDS – ČESKÁ LÉKÁRNA, A.S. (NETWORK OF DR. MAX PHARMACIES)

The inspection was concerned with performance of the duties of a personal data controller or processor in relation to processing of customers’ personal data within the network of Dr. Max pharmacies in cases where the customers use a Dr. Max client card.

The company processes the personal and sensitive data of its clients who use Dr. Max client cards in a database related to the FaRMIS software, which the company uses for the performance of its duties following from Act No. 378/2007 Coll., on pharmaceuticals.

Based on the client’s application for a Dr. Max client card and further processing of the data within the Dr. Max client card, the company obtains personal and sensitive data with a view to their further storage on a data carrier and also further processes the information. The company keeps a database of the personal and sensitive data of clients with a Dr. Max client card that is accessible to the employees of the given pharmacy that issued the client card to the

client. The data are stored in the database in a form allowing for their further processing, i.e. assignment of further data on medicines and health supplements dispensed.

In respect of issue and administration of Dr. Max client cards, the company referred to keeping of clients' pharmacy cards as the purpose (objective) of processing the personal and sensitive data of its clients. The company utilises the data from the pharmacy card to check interactions of the dispensed medicines, to check contraindications of medicines based on the provided data on diagnoses, to monitor allergic reactions to medicines and provide for their timely detection among the administered medicines, to seek unsuitable combinations and side effects in administration of medicines or combinations thereof, to inform the clients of news and developments in the area of health care and to provide bonuses for the collected medicines.

Clients with Dr. Max client cards are acquainted with the purpose of processing personal and sensitive data upon signature of the application to the client programme. The application includes the provision of the client's consent to personal data processing according to the requirements of the Personal Data Protection Act; the client confirms the application by his/her signature.

It was verified within the inspection whether the company had adopted sufficient organisational and technical measures within the meaning of Article 13 of the Personal Data Protection Act so as to avoid any unauthorized or accidental access to their personal data, or their change, destruction or loss, unauthorised transfers, other unauthorised processing, as well as other misuse of these personal data. It was ascertained in the inspection that the company had not breached the duties following for it from the Personal Data Protection Act.

Furthermore, the Office checked the company's procedure in dealing with applications of the data subjects for destruction of personal data in conformity with Articles 20 and 21 of the Personal Data Protection Act. Based on the ascertained facts, it was concluded that the company had violated Articles 20 and 21 of the Personal Data Protection Act by not destroying client's personal data without delay although the client had requested the destruction of his personal data and cancellation of his Dr. Max client card. It was ascertained in the inspection that the company had failed to carry out the said destruction for the reason of insufficient training of the personnel as to how they should proceed in cases where the client requests that his or her Dr. Max client card be cancelled. However, the company remedied the said shortcoming during the inspection.

In view of the findings of the inspection and the remedy of the procedure in destruction of clients' personal data, no remedial measures were imposed on the company.

INSPECTION CONCERNED WITH THE SUBMISSION OF DATA ON PATIENTS WITHIN SCREENING OF ONCOLOGY DISEASES

Based on an instigation, an inspector appointed by the Office performed an inspection in the Institute of Biostatistics and Analyses of Masaryk University in Brno (hereinafter "IBA MU"), concerned with compliance with the duties of a personal data controller stipulated by the Personal Data Protection Act in relation to gathering and processing personal data with a view to administration of data in monitoring of oncology screening programmes.

It was ascertained in the control that the screening programmes (screening of colorectal cancer, breast cancer and cervical cancer) were initiated on the basis of EU Council

Recommendation No 2003/878/EC of 2 December 2003 on cancer screening and were gradually implemented in co-operation with the Czech Society for Oncology. The legislative framework (scope and methodology) for the performance of screening has been gradually modified to the current version by decrees and Bulletins of the Ministry of Health of the Czech Republic.

Based on the ascertained facts, the inspectors noted that the data collected within the aforesaid screening programmes were not sufficient to identify the persons concerned and that these data were therefore not personal data within the meaning of Article 4 (a) of the Personal Data Protection Act.

Subsequently, a representative of IBA MU sent a written request to the Office for its opinion on the possibility of using IDs in the form of a unilateral imprint of the birth identification number created through a hashing algorithm under the condition of compliance with specific security measures.

Based on the written inquiry from the IBA MU representative, the Office advised him that if individual medical facilities sent data to the central storage of screening programmes modified in such a way that the option of any further identification of the patients concerned would be available only and solely to the medical facilities sending the data, while the operator of the central storage would not be able to directly or indirectly identify the specific patients in any way and if IBA MU as the operator of the central storage processed the accepted data only for its own, statistical, analytical, etc. purposes, it could be stated that the said method would be analogous to the method of processing that was the subject of the previous inspections described in the inspection protocol, and in that case the described method of using an unambiguous identifier consisting in the said imprint of the birth identification number with a hashing algorithm and other safeguards could not be considered a procedure constituting personal data processing in the sense of the Personal Data Protection Act.

Furthermore, the Office advised IBA MU that if the process took place in the manner in which it is described in the preceding paragraph, it could be stated that the operator of the central data storage for screening programmes would not be in the position of personal data controller in the sense of the Personal Data Protection Act, as it would not have access to information that it could directly or indirectly assign to specific natural persons, and this would thus not constitute personal data according to the definition set out in Article 4 (a) of the said Act. The Act as a whole will thus not apply to its activities.

CONTROL OF KEEPING MEDICAL RECORDS IN A HEALTH-CARE FACILITY

Based on an instigation, an inspector appointed by the Office performed an inspection at an eye clinic (hereinafter the "Clinic") that indicated a possible violation of Article 13 of the Personal Data Protection Act, which might have been committed by the data controller, i.e. the medical facility.

In the instigation, the complainant stated that, in her opinion, the Clinic breached the duties following from the Personal Data Protection Act, particularly the duty to adopt measures to avoid unauthorised or accidental access to personal data, their modification, destruction or loss, unauthorised transfers, other unauthorised processing, as well as other misuse of personal data, and also the duty to process only accurate data and the duty to process only personal data corresponding to the set purpose and within the scope necessary for attaining the set purpose. In the opinion of the complainant, the Clinic processed her

personal data at variance with her right to preservation of human dignity and at variance with the protection of her private and personal life.

The inspection demonstrated that the Clinic had breached its own internal regulation concerning the methods of keeping medical records, whereby it had breached Article 13 (2) of the Personal Data Protection Act by failing to adopt adequate technical and organisational measures, and had also violated Article 5 (1) (c) of the Personal Data Protection Act, and Article 67b (4) of Act No. 20/1966 Coll., because it had failed to keep accurate data on health care provided to the complainant at the Clinic.

The Clinic was required to take remedial measures consisting in the duty to adopt measures to ensure that personal data of the patients kept in the medical records pursuant to the special law were kept in the sense of Article 5 (1) (c) of the Personal Data Protection Act and to supplement the internal regulation so that it contained technical and organisational measures applicable in cases where medical records were handled directly by the examining doctor when the records were perused by the patient or authorised person.

The Clinic subsequently informed the Office that it had performed the remedial measures.

INSTIGATION AGAINST THE GENERAL HEALTH INSURANCE COMPANY OF THE CZECH REPUBLIC

The Office received an e-mail instigation aimed against the General Health Insurance Company of the Czech Republic (hereinafter "GHI") with a request for investigation whether GHI could publish data on debtors on its website (www.vzp.cz/platci/dluznici).

The inspector appointed by the Office analysed the instigation, which she subsequently set aside on the grounds that while it was true that, in terms of the Personal Data Protection Act, data pertaining to a natural person constituted personal data in the sense of Article 4 (a) of the Act, the GHI was authorised to process personal data of data subjects with a view to disclosing information on debtors within public health insurance in the sense of Article 5 (2) (a) of the Personal Data Protection Act, i.e. without consent of the data subject, because pursuant to Article 23 (3) of Act No. 592/1992 Coll., on premiums for general health insurance, as amended, the duty to maintain confidentiality pertaining to employees of a health insurance company did not apply to data concerning outstanding premiums, including the amount of outstanding premiums, in respect of which a decision had been made through a final payment assessment, or if this was a claim for premiums and penalties that the health insurance company enforced in a public auction or that had been ascertained in insolvency proceedings pursuant to a special legal regulation.

The complainant was informed of this opinion by the inspector of the Office.

INSPECTION CONCERNED WITH PERSONAL DATA PROCESSING IN RELATION TO THE USE OF PASSIVE IDENTIFICATION BRACELETS FOR PATIENTS – NA HOMOLCE HOSPITAL

It was ascertained within the inspection that the hospital was using passive identification elements – bracelets containing information marked thereon in the form of a sticker printed out of the hospital's information system.

The information on the bracelet is one of the basic means of assuring quality and safety of the patient during his/her stay in the hospital. Through control of the data on the identification

bracelet, it is ensured that a patient is not mistaken for another patient or that the results of his/her examination are not assigned to records of some other patient. This information plays an absolutely fundamental role in the performance of diagnostic or medical outputs, particularly outside the relevant department where the patient is hospitalised (imaging examination techniques, laboratory tests, surgery, etc.). They play an irreplaceable role in identification of disoriented and confused patients and patients under the influence of medicines (general anaesthesia, etc.). All the data marked on the bracelet are automatically also set out on each sheet of the medical records. Bar code readers are located next to computers providing access to NIS (rooms where health care is provided, i.e. departments, surgeries, etc.). The bar code on the bracelet can be read only from a distance of approx. 10 to 20 cm subject to direct visibility, which excludes the possibility of monitoring the patient's movement on the premises of the hospital.

With a view to publishing a recording from a medical output on the internet and, at the same time, for publication of data within the scope of the patient's birth identification number, name and part of the surname, during the inspection, the hospital presented the patient's "Consent to use of the performed diagnostic/medical output in the media" signed by the patient, which also included explicit consent to the use of the name, surname, date of birth, birth identification number, text information, video and audio recordings of the given person or parts of his/her body and also a manifestation or other elements of personal nature. The controlled entity further stated that this record had already been removed from the website since the hospital had never actually intended to publish the birth identification number of the given patient, in spite of having written consent of the patient to this effect.

The inspection revealed no breach by the hospital of its duties as personal data controller in processing of personal data according to the Personal Data Protection Act.

CAMERA SURVEILLANCE SYSTEM

SUPERIOR STATE ATTORNEY'S OFFICE IN PRAGUE

An inspection of the Superior State Attorney's Office in Prague was carried out based on an instigation from the President of the Office. The aim was to assess compliance with the duties stipulated for the Superior State Attorney's Office in processing of personal data obtained through the camera surveillance system operated by the controlled entity at its seat.

On 24 February 2012 the Superior State Attorney held a press conference where he displayed to the journalists recordings from the camera surveillance system of 17 February 2012 and added his commentary.

Within the performance of the duties following from the Personal Data Protection Act, the Superior State Attorney's Office had issued two internal regulations, specifically Measure of the Superior State Attorney' in Prague No. 4/2011 to secure protection of personal data in the operation of a camera surveillance and recording system and the Principles of Data Protection in the System at the Superior State Attorney's Office in Prague.

The inspection revealed a difference between the period of maintenance of recordings registered with the Office and the period for which the recordings were actually maintained, which was caused by the set quality of the stored recording, depending on the size of the stored data. The equipment does not allow for time loop setting. The period of the recording was estimated for the purposes of registration by the supplier of the equipment.

Based on instigation of his subordinate employee, the Superior State Attorney used his authorisation to access the recordings from the camera surveillance system and saved copies of these recordings on his PC in his office.

The inspector ascertained breach of the duties following from the Personal Data Protection Act in respect of its Articles 13 (3) and 16 (1). While the controlled person adopted measures to secure personal data, he did so inconsistently, which is clearly indicated particularly by the finding made by the Superior State Attorney that the recordings were five days old (rather than three days) and by an extract from the audit records/logs that were demonstrably assessed by no one until the date of commencement of the inspection. Furthermore, it cannot be unambiguously determined which of the authorised persons used the system. The controlled entity also failed to perform the reporting duty as it did not notify the Office of the ascertained difference between the period of actual storage and the period registered with the Office.

The inspection findings were reflected in remedial measures imposed by the inspector. The Superior State Attorney's Office in Prague accepted the results of the inspection and submitted to the Office a report on implemented remedial measures.

However, the findings also indicated misconduct on the part of an employee of the controlled entity, i.e. a person authorised to work with the system. The inspectors came to the conclusion that by publishing images from the camera surveillance system, the Superior State Attorney breached his non-disclosure duty as the publication did not conform to the purpose for which they were intended.

This violation of the Personal Data Protection Act was then dealt with in administrative proceedings pursued by the Office. The decision of the Office had not entered into legal force by the end of 2012.

CAMERA SURVEILLANCE SYSTEM ON BUSINESS PREMISES

Investigation on site revealed that the controlled entity installed a camera surveillance system on its premises with the use of an external contractor. According to information provided by the complainant, the controlled entity thus monitored all the activities performed on surrounding properties. The reason for installing the camera surveillance system lay in the protection of the controlled person's property. The control unit with a monitor is located in the office of the establishment. The camera surveillance system consists of four cameras. At the same time, one mock-up camera is installed on the outer wall of the building. The camera recordings are stored on the control unit's hard disk. The camera surveillance system continuously records colour images. It lacks the zoom function and the cameras are not mobile (turning). The period of storage depends on the available capacity of the hard disk. The capacity of the disk is sufficient for approx. 10 to 14 days of recordings. Neither the business premises nor its inner areas are marked with any information sign concerning the operation of the camera surveillance system.

During the oral hearing and on-site investigation, it was agreed with a representative of the external contractor that they would change the angle of view of one of the cameras so that it monitored exclusively the property of the controlled entity and notify the Office of this fact without delay.

At the time of commencement of the inspection, the controlled entity was not registered in the register of personal data controllers kept by the Office.

The inspection was closed with the following conclusion: the period of 10 to 14 days for which the recordings made by the camera surveillance system were maintained did not correspond to the necessary period of time; the controlled entity would learn of any extraordinary event captured by the camera surveillance system not later than on the following business day.

A personal data controller is obliged to inform the data subjects in gathering personal data to what extent and for what purpose the personal data will be processed, who and in what manner will process the personal data and to whom the personal data might be disclosed unless this information is already available to the data subject. The controller must inform the data subject of his/her right to access the personal data, the right to have personal data rectified, as well as other rights stipulated in Article 21 of the Personal Data Protection Act. In view of the fact that the controlled entity does not inform third parties, at least by means of an information sign, that personal data are being gathered on the premises by means of a camera surveillance system, the less so of other requisites of personal data processing, it breaches the duty imposed thereon as a personal data controller in Article 11 (1) of the Personal Data Protection Act.

Based on the ascertained facts, the controlled entity was required to adopt remedial measures as follows: to comply with the duty to inform data subjects pursuant to Article 11 (1) of the Personal Data Protection Act, by means of installing information signs on the monitored premises, and at the same time inform the data subjects of other requisites of personal data processing pursuant to Article 11 (1) of the Act, at least by means of a written notice displayed on the premises; and not to maintain personal data gathered through the camera surveillance system with recording equipment for a term that is not essential for attaining the set purpose.

CAMERA SURVEILLANCE SYSTEM IN A SOCIAL CARE FACILITY

For the first time over the six years of existence of the Public Relations Department, the trend The inspection revealed that, in the building where it provided its social services, the organisation had installed a camera surveillance system with a view to protection of persons against attack by an aggressive person, protection of property against theft, as well as any other unlawful or criminal activity, and also in the interest of preventing undesirable phenomena, particularly destruction of common property and vandalism.

In the given case, the processing of personal data through the camera surveillance system does not infringe on the rights of data subjects (employees, clients, visitors, etc.) to protection of their private and personal lives.

However, at variance with the set purpose, the recording was used to investigate a client's complaint and the organisation thus breached its duty to process personal data only in conformity with the purpose for which they had been gathered.

It may process personal data for another purpose, i.e. use the recording, only if the data subject has given its consent to this effect. Since the controlled entity did not have such consent available and, furthermore, had breached its reporting duty to the Office before processing of personal data through the installed camera surveillance system, the inspector noted violation of the Personal Data Protection Act and a fine was imposed on the organisation.

MUNICIPAL CAMERA SURVEILLANCE SYSTEM

The inspection was concerned with personal data processing through the city's camera surveillance system, and the relevant guidelines and procedures in utilisation of recordings from the city's camera surveillance system.

An instigation for the inspection was submitted to the Office by a district department of the Police of the Czech Republic.

The Police of the Czech Republic provided the files collected on the basis of investigation of a criminal complaint related to abuse of official powers (unauthorised surveillance of the complainant by the camera surveillance system and making an audio recording of his complaint against the conduct of a municipal police officer), which had allegedly been committed by the Director of the Municipal Police and Deputy Mayor of the City in obtaining evidence on unlawful conduct of the complainant in hearing his breach of traffic regulations. The complainant learnt about the alleged unlawful conduct of the Director of the Municipal Police and Deputy Mayor of the city in relation to his criminal prosecution on the grounds of his attack against an official (public officer), which the complainant had allegedly committed during hearing of his traffic infraction by the municipal police.

The inspector closed the control with the conclusion that the personal data and recordings from the camera surveillance system collected in public areas of the city, within the scope ascertained in the inspection, unambiguously contributed to the set purpose and that the recordings were not processed beyond the scope of the set purpose, consisting in protection of property and health of citizens and property of the city and other entities. In the given case, the Office considers the period of three to ten days for which the recordings from the camera surveillance system are stored to be an admissible period for which the personal data can be stored in the recording equipment for the set purpose.

The inspector is of the opinion that the recordings involving the complainant (and other persons) were made and stored in accordance with a public interest that outweighed, in the given case, the interest in protection of the complainant's private and personal life. It was not proved that the controlled entity had processed the recordings without authorisation or had otherwise misused them, thus interfering with the private and personal life of the complainant.

In the conclusion of the inspection, the inspector appointed by the Office noted that the city had not violated the Personal Data Protection Act in relation to processing of the complainant's personal data through the city camera surveillance system. For this reason, no remedial measures were imposed.

PRAGUE AIRPORT – INSPECTION CONCERNED WITH PERSONAL DATA PROCESSING WITH THE USE OF RECORDS FROM CAMERA SURVEILLANCE SYSTEMS INSTALLED IN PUBLICLY ACCESSIBLE AREAS OF THE AIRPORT

As of the date of the investigation on site, 1226 cameras were installed on the premises of the Airport to monitor the interior premises of the Airport where passengers and other persons are present, and furthermore monitoring the interior premises of the Airport where operating technology is located, outer public areas in front of the Airport, the airfield and areas of parking lots and parking houses (with a system of identification of the licence plates). The camera surveillance system with recording equipment is operated continuously, 24 hours a day, 7 days a week, and the recording is also made continuously.

At the same time, the Airport operates a system of recognition of licence plates of vehicles in short-term parking lots (hereinafter the "Parking System"). For the purposes of controlling the operation of short-term parking lots in front of the terminals and, where appropriate, collecting the parking fees, the Airport uses a system for control of entry to and exit from the parking lots based on electronic recognition of the licence plates of motor vehicles.

In conclusion, the inspector performing the inspection noted that, with a view to ensuring, in particular, safety and protection of air transport, the Airport used a CCTV system with recording equipment and was therefore the controller of personal data obtained from the CCTV system. For controlling the operation and collection of fees in short-term parking lots, it used the Parking System based on scanning and recognition of licence plates. The Airport is therefore the controller of personal data obtained in the Parking System. Based on these findings, the inspector concluded that the technical and organisational measures adopted by the Airport were sufficient to fulfil the duties stipulated by Article 13 of the Personal Data Protection Act. According to the internal guideline for handling CCTV recordings, data are exported from the CCTV system (permanent storage on a portable data carrier) in two copies, where one copy is intended for applicants for data export and the other for keeping records, without specification of the period for which the exported data are to be filed and without specification of the purpose of filing. Within the investigation on site, the controlled entity stated that the exported recordings from the CCTV system were filed permanently without any time limitation, and that the purpose of maintaining these recordings was to resolve any potential conflicts with applicants for data export, clarification of potential abuse of the exported data and other similar situations. In view of the fact that the purpose of permanent filing of recordings exported from the CCTV system is not explicitly stipulated in the internal guidance documents and, at the same time, such filing is not covered by Article 5 (1) (e) of the Personal Data Protection Act ("*After expiry of this period, personal data may be maintained only for the purposes of the State statistical service, for scientific purposes and for archiving purposes.*"), the inspectors concluded that permanent storage of the recordings exported from the CCTV system was at variance with Article 5 (1) (e) of the Personal Data Protection Act.

Pursuant to Article 11 (1) of the said Act, the controller has the following duty: "*A personal data controller is obliged to inform the data subjects in gathering personal data to what extent and for what purpose the personal data will be processed, who and in what manner will process the personal data and to whom the personal data might be disclosed unless this information is already available to the data subject. The controller must inform the data subject of his right to access the personal data, the right to have personal data rectified, as well as other rights stipulated in Article 21*". Information signs are installed at entrances to the airport terminals with a pictogram of a camera and the text "THE PREMISES ARE MONITORED BY A CAMERA SURVEILLANCE SYSTEM". According to the inspector, this information is not sufficient to comply with the duties of the controller pursuant to Article 11 (1) of the Personal Data Protection Act.

In relation to the operation of the Parking System, the inspector recommended to the Airport that, in cases where the drivers do not breach the applicable Rules of Operation, it store the images of licence plates of vehicles as well as the data processed in this relation only for the period that is necessary in the sense of the set purpose, i.e. to provide for the operation and collection of fees at the parking lots in conformity with the applicable Rules of Operation and the Price List, but not exceeding 24 hours.

An information sign is installed on a pole next to the entrance to the parking lot with a pictogram of a camera and the text "*THE PREMISES ARE MONITORED BY A CAMERA SURVEILLANCE*

SYSTEM". The scope of the thus-provided information must be considered inadequate in the sense of the above-cited Article 11 (1) of the Personal Data Protection Act.

Pursuant to Article 13 (4) (c) of the said Act, the controller or processor is also obliged, in the area of automated personal data processing, within the measures pursuant to paragraph 1 of the same Article, *"to acquire electronic records that allow for determining and verifying as to when, by whom and for what reason the personal data were recorded or otherwise processed"*. The Parking System application gathers and processes only operating data on the movement of vehicles in the parking lot and stores no other data, i.e. on access to the stored data and their subsequent processing. In the opinion of the inspector, by operating the Parking System application, the Airport thus fails to fulfil the duty imposed by Article 13 (4) (c) of the Personal Data Protection Act.

By processing personal data through the CCTV system with recording equipment, the Airport violated Article 5 (1) (e) and Article 11 (1) of the Personal Data Protection Act and, by operating the Parking System with recognition of licence plates of vehicles, the Airport violated Article 11 (1) and Article 13 (4) (c) of the Act. The inspector imposed on the Airport the duty to modify forthwith the information signs pertaining to the CCTV system at the entrances to the airport terminals so as to comply with the duty imposed in Article 11 (1) of the Personal Data Protection Act and the information signs on the CCTV system at the entrances to the short-term parking lots so as to comply with the duty imposed in Article 11 (1) of the Personal Data Protection Act, also in respect of the specific conditions of personal data processing through the Parking System. Furthermore, she required that the Airport ensure, within three months, that copies of the recordings from the CCTV systems ("exports") are maintained only for a period not exceeding 90 days, destroy within three months all copies of recordings from the CCTV system made to that date and kept beyond the set time limit, and provide within a deadline of six months for such modifications of the application software of the Parking System so as to comply with the requirements set out in Article 13 (4) (c) of the Personal Data Protection Act. At the same time, the Airport was required to provide the inspector with a written report on remedial measures adopted, without delay after implementation of each individual measure.

CAMERA SURVEILLANCE SYSTEMS IN AN APARTMENT BUILDING

The inspector appointed by the Office closed a repeated inspection of the camera surveillance system installed by an Association of Unit Owners (hereinafter the "AUO") in an apartment building in Přeborn, which was concerned with control of performance of remedial measures resulting from an inspection by the Office and set out in the inspection protocol of February 2010. The inspection was preceded by an inspection performed in 2009, which was closed in February 2010, with the following findings and legal assessment of violation of the provisions of the Personal Data Protection Act. The AUO breached the duty stipulated in Article 5 (2) of the said Act, i.e. the duty to process personal data with consent of the data subject and, without such consent, only on the basis of exemptions pursuant to Article 5 (2) (a) to (g) of the Act; the AUO breached the duty stipulated in Article 11 (1) of the Personal Data Protection Act, i.e. the duty to inform the data subjects of the scope in which and the purpose for which the personal data would be processed, by whom and in what manner the personal data would be processed and to whom the personal data could be disclosed, and failed to inform them of their right of access to personal data and the right to have their personal data rectified, as well as of other rights stipulated in Article 21 of the Act; the AUO violated Article 16 of the Personal Data

Protection Act, i.e. the duty to notify the Office for Personal Data Protection of the fact that it intends to process personal data prior to proceeding with the processing of personal data, and thus committed an administrative offence pursuant to Article 45 (1) (e), (f) and (i) of the Personal Data Protection Act, because it was processing personal data without consent of the data subjects in cases other than stipulated by the law, failed to provide the data subjects with information within the scope or manner stipulated by the law and failed to comply with the reporting duty pursuant to the Act.

In February 2009, the AUO raised objections against the inspection protocol. Within the proceedings on the objections, in May 2010 the President of the Office issued a decision in which he dismissed the objections raised by the controlled entity to the full extent.

The repeated inspection was initiated on the basis of a complaint made by two inhabitants of the building (hereinafter the “complainants”) in July 2011.

In conformity with Article 40 (1) of the Personal Data Protection Act, the inspector appointed by the Office imposed on the AUO measures to remedy the established shortcomings and set a deadline for remedy: not to gather and, furthermore, not to process personal data of persons present in the monitored areas of the building with the use of camera recordings from the CCTV system (at the entrance and in the area of post boxes) in a manner contravening the applicable legal regulations so as to minimise interference with the privacy of persons walking along the corridors on the ground floor of the apartment building and, at the same time, while maintaining or increasing the level of protection of the AUO’s property; not to gather and, furthermore, not to process personal data of persons in elevators with the use of camera recordings from the CCTV system in a manner contravening the applicable legal regulations; and to bring the information submitted to the public register of personal data controllers kept by the Office for Personal Data Protection in respect of consents to personal data processing into conformity with reality.

MANAGEMENT OF SENSITIVE PERSONAL DATA OF CLIENTS OF A RETIREMENT HOME AND PROCESSING OF THEIR PERSONAL DATA THROUGH A CAMERA SURVEILLANCE SYSTEM WITH CAMERAS INSTALLED IN THE ROOMS AND COMMON PREMISES

The inspection, which revealed breach of the Personal Data Protection Act in unauthorised management of personal and sensitive data of the clients of a retirement home pursuant to the Commercial Code, also revealed, in co-operation particularly with the Ombudsman, the suspicion that the retirement home was providing health services without having the necessary authorisation and that it was also providing these services without authorisation pursuant to Article 107 (1) of Act No. 108/2006 Coll., on social services, i.e. without registration, on which decision is to be made by the competent authority according to the registered office of the retirement home.

The results of the inspection proved that the retirement home processed personal data of the clients of the commercial accommodation facility by means of a camera surveillance system with recording equipment installed in rooms of the individual clients, in corridors and in the room marked “nurses station” at variance with the Personal Data Protection Act.

It is clear that making a camera recording within any scope for the reason of monitoring the development of health condition, or to protect the clients from falling from their beds, has no

purpose. Personal care by nurses, supplemented, in exceptional cases, by a camera surveillance system with on-line transmission, would be essential for attaining this purpose; however, this would be possible only in facilities providing health or social services pursuant to the special law. However, the controlled entity did not meet this condition and therefore a camera surveillance system with on-line transmission could not be recommended for this purpose. Camera recordings tend to have a documentation function and cannot serve the preventative purpose as stipulated by the controlled entity.

The controlled entity also did not have free and informed consent of the clients whose sensitive data it processed in their personal cards.

A fine was imposed on the retirement home for breach of the duties imposed by the Personal Data Protection Act; should another or repeated breach of the duties in similar business activities in some other establishment be found based on the results of an investigation pursued by the Ombudsman in relation to the suspected violation, particularly of Act No. 108/2006 Coll., on social services, another fine could be imposed in relation to the violation of the Personal Data Protection Act, including a fine for failure to comply with the imposed remedial measures.

■ ADDRESSING COMPLAINTS AND PROVISION OF CONSULTATIONS

Unlike in 2011, when the increase was not so marked, the Public Relations Department of the Office again recorded a steady increase in the number of instigations and complaints concerning unlawful conduct in personal data processing, which has been growing by approx. 20 % year-by-year in the long term. The Office received a total of 1319 pleadings; their number thus increased in total by 18 % compared to 2011.

This year the said trend has ultimately resulted in a state where all the pleadings can no longer be handled by the current personnel of the Office (and the number of inspectors cannot be increased), as it is not realistic to initiate almost one thousand ad hoc inspections in a single calendar year. In view of the experience gained by similar supervisory authorities in the European Union and based on the new European framework for personal data protection, which is currently under preparation, this should not even be the main subject of activities pursued by the Office.

After having evaluated the results of analysis of information obtained over the more than twelve years of its existence, the Office came to the conclusion that personal data protection is primarily up to data subjects themselves. The legal awareness of citizens in this area is constantly growing and has reached a level where the vast majority of them is able and willing to exercise their rights stipulated by the Personal Data Protection Act. These were the main reasons that led the Office to propose amendment to the cited law, which abolishes the citizens' right to address directly the Office without having previously at least attempted to resolve the matter by means of a written request for explanation, remedy of the defective state or blocking and destruction of their personal data, addressed to the given personal data controller. Only when their justified claims are not satisfied may they turn to the Office, while at least documenting the merits of the case, e.g. by copies of the relevant correspondence with the controller.

The said legislative change to the Personal Data Protection Act (abolishment of former Article 21 (4)) was the main reason for an increase (by 27 %) in the number of complaints set aside as unfounded. The numbers of instances when complaints were resolved in another way remained practically unchanged compared to the previous years, which is indeed at the very limit of the Office's capacity, particularly in respect of the number of complaints referred for inspection (approx. 200 per year).

Statistical data on complaints addressed in 2012

Total	1 319, of which:
referred for inspection	197
referred for initiation of proceedings	69
forwarded to the competent bodies	13
dismissed as unfounded	1 040

Similar to 2011, the greatest increase in the number of pleadings was recorded in the area of modern information technologies, which can be generally denoted as the area of Internet (547 pleadings). The area of social networks, particularly the globally most dynamically growing Facebook network, which is used by almost 1 billion people, as well as various discussion forums, "private" databases of debtors, persons not paying debts, etc., thus became, for the first time in history, the most frequent subject of complaints submitted by affected citizens.

A marked increase in the number of complaints by employees concerned with their unlawful monitoring at the workplace and in common areas of the employer's organisation was recorded in relation to the new Corporate Criminal Liability Act, which entered into effect on 1 January 2012. This no longer involves merely camera surveillance systems with recording equipment, but also abuse of increasingly sophisticated technical means for monitoring telephone calls, e-mail, hidden photo traps, deployment of systems utilising GPS and WiFi for localising employees, etc.

Based on analysis of this type of pleadings, it is possible to conclude that the employers are well aware of the risks that may be caused by an irresponsible employee, including deletion of the company from the Commercial Register. They knowingly exceed the statutory authorisations with a view to choosing absolutely reliable employees and to controlling and monitoring them, again often outside the law, at the workplace, in common areas and even outside working hours.

Protection of personal data processed within labour-law relationships constitutes a major part of the Office's supervisory activities. Its mission is primarily to protect data subjects, i.e. employees, against unauthorised or otherwise unlawful processing of personal data. At the same time, the Office strives to be absolutely impartial also in terms of its approach to the justified interests of employers in the position of personal data controllers. Within its administrative discretion, it can reflect and respect that the basic interest of employers is to attain profit and have prospects for further development of their companies in free operation of business, but naturally only within the limits of the Personal Data Protection Act as a law providing for a fundamental human right. Incorrect procedure of "obliged entities", mostly municipal authorities, consisting in publication of personal data of parties making an inquiry pursuant to the Free Access to Information Act was a phenomenon consistently

occurring in 2012 (for more details, see the chapter of this Annual Report “Right to information while respecting the right to personal data protection”).

The Office strived to introduce a systemic solution in co-operation with the substantively responsible authority, i.e. the Ministry of the Interior, which issued a methodical instruction for all public administrative authorities in this respect. A similar problem occurred in courts of all instances and, again, as it would be highly ineffective to deal with each case separately ad hoc, the President of the Office wrote a letter to the Minister of Justice, who in turn promised to provide for a remedy, again by issuing a methodical instruction aimed at eliminating the said undesirable practice.

The Office received a number of requirements from public administrative authorities and non-governmental organisation in relation to video and audio recordings made at meetings of municipal assemblies. At the present time, the Office is preparing a separate position on this issue, although it already provided interpretation in its Annual Report for 2011. It can therefore only be stated in this respect that the Office must respect the applicable laws, particularly the Municipal Act, which continues to distinguish two categories of persons in terms of access to the minutes of meetings of the municipal assembly, and thus also to the recordings made at the meetings - in principle, citizens having a permanent address in the municipality, to whom the minutes are disclosed to the full extent, and others who do not have the right to access the minutes pursuant to the Municipal Act. There has been a shift in the approach by municipal authorities, which now tend to refrain from making recordings and provide on-line transmissions of the meetings of their assemblies. While this activity is outside the competence of the Office, as it does not involve personal data processing within the meaning of the Personal Data Protection Act, nonetheless, publication of the entire course of the meeting to an unlimited circle of persons is no fundamental improvement in terms of potential interference with privacy of citizens. The same opinion was also presented by the Ombudsman in Information Bulletin of the Office No. 2/2011, dedicated to camera surveillance; consequently, more than a year ago, the Ombudsman recommended to adopt appropriate legislative measures.

The following belong among the most frequent and, at the same time, most serious violations of the Act by controllers and processors of personal data determined in 2012: failure to adopt appropriate measures to secure the personal data being processed, their unauthorised gathering, publication and other forms of processing without consent of the data subject. The Office will continue to focus its attention on these cases.

■ FINDINGS OBTAINED IN ADMINISTRATIVE PROCEEDINGS

“ FALSE ” CONTRACTS

More frequently than in the previous years, in 2012 the Office encountered agreements on the provision of various types of services (and less often, purchase contracts) for which personal data of data subjects had been used without authorisation and without their knowledge. This constitutes violation of the Personal Data Protection Act. It is typical of these cases that the

agreements were not concluded directly between the interested party and the service provider, but rather through various agents. The agent often works as a natural person operating a business for a certain company (or for another natural person operating a business) where only the latter has a contract concluded with the service provider himself. The relationships among the individual persons and the related responsibility for personal data protection thus become highly obscured.

Instigations for investigation into this area are usually submitted to the Office by the Police of the Czech Republic, which pursue their own investigation based on a criminal complaint lodged by the alleged client, who has learnt of the misuse of his/her personal data in some way – typically when the alleged client was addressed by the service provider with a request for payment. In certain cases, the criminal complaint is lodged by a service provider who is alleged to be a party to a false contract, again based on instigation from a client who confronts the provider when certain financial performances are being claimed from him/her. The prosecuting bodies usually conclude that the act in question does not correspond to the elements of a criminal offence, particularly because it lacks the required social harmfulness, or because the amount of damage is not sufficient for this to be an offence pursuant to the Criminal Code. Indeed, in most cases, the agreement is cancelled without any difficulties by the service provider based on a request of the given data subject and the alleged client usually loses time rather than money. These acts are then discussed as administrative offences in the area of personal data protection. The highest penalty imposed by the Office in these cases to date was a fine of CZK 50,000.

It is also worth mentioning that, as follows from the cases set out below, the agent is not always driven by an intention to obtain an unjustified commission. However, this motive is certainly most frequent. In some of the ascertained cases, the objective was to “merely” achieve the required number of concluded contracts and the agent clearly counted on being able to cancel the contract before the alleged client learns about the unauthorised use of his/her data.

It is also important to note that, in a majority of cases, the set of personal data used without authorisation includes a birth identification number as the general identifier of citizens. As a result of excessive use of this data in private-law relationships, which is often criticised by the Office, a contract containing the birth identification number of the service recipient does not automatically become, quite paradoxically and contrary to the expectations of the other party, more accurate and reliable.

It must be emphasised that the service provider for whose benefit the contracts are concluded is also always obliged to prevent the conclusion of “false” contracts by appropriate setting of its internal processes. A possible method of detecting problematic contracts as soon as possible could lie, for example, in sending a “welcome letter” to all new clients with a summary of the contents of the executed contract. The fact that when contracts executed by a certain agent without authorisation are found, it is necessary to consistently check all the other contracts concluded by the same agent, should be self-evident. Should the direct service provider (or his agent with whom the agent that concluded the dubious contract co-operates based on their mutual agreement) fail to do so, he must be deemed partially liable, also in terms of personal data protection.

The description of the specific cases clearly indicates that certain circumstances keep recurring. This includes, for example, the fact that the data were obtained from bills that the data subject himself showed to the agent, because the latter had offered him financially more

advantageous services. The Office must therefore join various consumer organisations in their repeated warnings against contracts concluded on the stairs or on the doorstep (the same is true of “mere” submission of underlying documents for potential later execution of such a contract).

The following should be added to this subject in conclusion: *In view of the above-described unlawful practice that is becoming increasingly frequent, the Office will be forced to deal with this area in all parts of its supervisory activities. Indeed, it seems necessary to focus not only on the ascertained cases of violation of the Personal Data Protection Act in response to detected offences, but also on prevention of these practices. Such a proactive approach will certainly also benefit from control activities involving assessment of measures taken by service providers to detect contracts concluded without authorisation. Furthermore, the Office will have to consistently evaluate the seriousness of the conduct of the person committing the administrative offence and the amount of the ensuing penalty, although it is convinced that the aforesaid conduct is primarily a question of breach of civil- or commercial-law relationships. However, interferences with the privacy and the right to protection of personal data may in no case be overlooked.*

PUBLICATION OF INFORMATION (PHOTOGRAPHS OR PARTS OR RECORDINGS) OBTAINED WITH THE USE OF A CAMERA SURVEILLANCE SYSTEM WITH A VIEW TO DETECTING OFFENDERS

The year 2012 witnessed a highly controversial public debate related to several proceedings pursued by the Office in respect of publication of information by private persons with a view to identifying persons committing unlawful conduct (infractions or criminal offences). This included especially publication in social networks (or generally on the internet) of photographs made by camera surveillance systems installed at places where unlawful conduct allegedly occurred.

Assessment and balancing of two criteria – the right to protection of property and the right to privacy – is fundamental for evaluation of legality of a majority of camera surveillance systems. In fact, one of the basic properties of a camera surveillance system is that, in the vast majority of cases, it gathers and maintains personal data, i.e. information on private life, on normal people who commit no unlawful conduct. It is therefore possible to operate camera surveillance systems without consent of the data subjects only if it is unconditionally secured that the personal data from the camera surveillance system will not be published or otherwise disseminated.

However, in a democratic state governed by the rule of law, identification of persons who have committed a criminal offence and collection of evidence on their guilt is the task of prosecuting bodies (i.e. bodies of the State), rather than of the operator of a camera surveillance system. Each controller of personal data from a camera surveillance system is therefore authorised, in conformity with the purpose of protection of property, only to submit the recording to the prosecuting bodies, but may not himself publish the recording. Under the conditions stipulated by the law, based on their knowledge and experience, and after having evaluated all the available evidence and information, the prosecuting bodies may initiate criminal proceedings against a specific person, which is a manifestation of the fact that the given person is justifiably suspicious of committing a crime, or launch a search for this person.

■ FINDINGS FROM COURT REVIEW

The Office for Personal Data Protection is a party to a great many court proceedings. As far as findings from the decision-making practice in 2012 are concerned, mention should be made of five important areas related to **tax administration, the nature of an instigation or complaint by the data subject, consent of the data subject to personal data processing, the notion of commercial communication and operation of camera surveillance systems.**

TAX ADMINISTRATION

Frequent arguments related to the actual application of the Personal Data Protection Act in the area of tax administration refer to the exemption embodied in Article 3 (6) (f) of the Personal Data Protection Act, according to which Articles 5 (1), 11 and 12 do not apply to processing of personal data necessary for the performance of the controller's duties stipulated by the special laws in pursuit of an important financial interest of the Czech Republic or the European Union, including, in particular, the stability of the financial market and currency, functioning of money circulation and payment relationships, as well as budget and fiscal measures.

In the statement of reasons for its judgment file No. 11 Ca 91/2009 of 5 June 2012, the Municipal Court in Prague stated that *"it cannot be stated in general that the Personal Data Protection Act does not apply to tax proceedings."* The assessment of whether the said exemption applies to a certain situation in view of an important financial interest of the Czech Republic should be made in co-operation with the Office for Personal Data Protection and the competent tax authority.

It has also been argued in the said context that the tax rules contain a special autonomous legal regulation of confidentiality, affording a higher level of protection to all data being processed and *"that the non-disclosure duty borne by the tax authorities is limited in a situation where the tax authority is requested to provide data by an entity authorised to obtain such data, which in the given case ... is the Office for Personal Data Protection, which is authorised to become acquainted with personal data and is also bound by the duty to maintain confidentiality."*

PERFORMANCE OF SUPERVISION

A petitioner is not entitled to claim that the Office exercise its supervisory competence and the relevant pleading is thus merely an instigation to exercise the Office's supervisory rights, where information from the Office on the manner of resolving an instigation is merely a communication from the Office, rather than a decision pursuant to Article 65 of Act No. 150/2002 Coll., the Code of Administrative Justice.

FAILURE OF THE DATA SUBJECT TO EXPRESS DISAGREEMENT WITH PERSONAL DATA PROCESSING CANNOT BE CONSIDERED CONSENT PURSUANT TO ARTICLE 4 (N) OF THE PERSONAL DATA PROTECTION ACT

In a case that ultimately resulted in a judgment rendered by the Municipal Court in Prague, the court assessed processing of personal data of a job seeker, which continued after the end of the selection procedure for the vacancy without express consent of the data subject.

UNSOLICITED COMMERCIAL COMMUNICATIONS

An individual response to a specific offer is not an unsolicited commercial communication pursuant to Act No. 480/2004, on certain services of the information society and on amendment to certain laws (the Act on Certain Services of Information Society) and the same is true of a specific counterproposal in reaction to an offer following from an advertisement.

EXTENSIVE AND UNDIFFERENTIATED USE OF A CAMERA SURVEILLANCE SYSTEM IS AT VARIANCE WITH ARTICLE 5 (2) (E), THE PART OF THE SENTENCE AFTER THE SEMICOLON, OF THE PERSONAL DATA PROTECTION ACT, WHICH REQUIRES THAT THE RIGHT OF THE PERSONS BEING RECORDED TO PROTECTION OF PRIVACY AND PERSONAL LIFE BE MAINTAINED

In the judgment, the Municipal Court in Prague stated that where a camera surveillance system is used extensively, i.e. where it simply monitors the premises where the clients of a hotel are present, rather than being, e.g. focused on objects that could be the aim of unlawful conduct (such as places intended for storage of things), the specific manner of obtaining camera recordings cannot be deemed to comply with the requirement of Article 5 (2) (e), the part of the sentence after the semicolon, of the Personal Data Protection Act, i.e. respecting the right of the persons being recorded to the protection of privacy and personal life.

The said manner of installation of the camera surveillance system is, in the court's opinion, clearly disproportionate. Indeed, the interest in protection against minor thefts, vandalism and potential unlawful conduct by a certain party cannot automatically outweigh the interests in protection of privacy and personal life.

■ REGISTRATION

The trend of increasing number of registrations notifications continued in 2012. During the year, the Office received 5169 notifications of processing data pursuant to Article 16 of the Personal Data Protection Act. This marks a 17% increase compared to the previous year. In connection with the increasing number of registration notifications, there has also been an increasing number of notified changes and supplements to previously registered instances of processing. The changes are most frequently concerned with addresses, supplementation of the scope of the processed personal data, categories of data subjects and supplementation of the purposes of processing. The Office received 811 applications for a change or supplementation in 2012.

In addition to assessment of registration notifications received, the Office issues decisions on cancelling registration pursuant to Article 17a (2) of the Personal Data Protection Act. A total of 78 instances of processing were thus cancelled this year 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. This was an increase by 59 %. The Office compulsorily publishes information on cancelled registrations in its Journal. Where the notice does not contain all the requisites required for actual assessment of the processing,

the controller is sent a request to supplement the information. In 2012 the Office initiated a total of 969 proceedings on registration pursuant to Article 16 (4) of the Personal Data Protection Act. In a majority of cases, the proceedings were concerned with processing via camera surveillance systems, processing of sensitive data and processing of personal data without legal grounds. If a justified concern about violation of the law arises or continues during the proceedings, the Office initiates administrative proceedings in the sense of Article 17 of the Personal Data Protection Act, which may result in a decision not to permit the notified processing.

Directive 2007/66/EC of the European Parliament and of the Council was transposed to the Czech legislation through Act No. 468/2011 Coll., amending Act No. 127/2005 Coll., on electronic communications and on amendment to certain related laws (the Electronic Communications Act), as amended. [HYPERLINK "http://www.uoou.cz/files/127-2005.pdf"](http://www.uoou.cz/files/127-2005.pdf) \t "_blank" \o "Odkaz na PDF soubor, velikost 714kB" The amendment, which entered into effect on 1 January 2012, introduces a new instrument for protection of personal data and privacy. The providers of electronic communication services are explicitly required to deal with data breaches, including the duty to notify such a breach to the Office for Personal Data Protection. A special section was created within the Office's website in relation to the new competence ("Notifications pursuant to Act No. 127/2005 Coll."), including links to legal regulations, a form for the performance of the notification duty and also definition of certain terms and procedures required of the notifier.

The registration department has received several pleadings in relation to the new duty imposed by the Electronic Communications Act on the providers of electronic communications. However, in a majority of cases, these pleadings were made by a data subject in respect of suspected breach of the duties imposed on a personal data controller by the Personal Data Protection Act, and they were thus referred to the competent department for resolving. The Czech Republic has yet to gain any substantial or thorough experience with these cases.

However, there have already been certain examples of notified breaches of personal data protection:

- personal data sent to a wrong addressee (e.g. by e-mail or letter);
- theft or loss of hardware with personal data;
- disclosure of personal data to unauthorised persons (backup of data on P2P networks, imperfect deletion of records in second-hand equipment for sale, use of "valid" data in testing new applications, unsuitable storage of login data or incorrect setting of the system and applications);
- loss or incorrect destruction of printed documents with personal data;
- hacker attacks (attacks aimed against a website, internal information systems, communication networks);
- results of attack by harmful programmes leading to breach of personal data protection (inaccessibility of data, publication of data, etc.).

Special types of processing carried out through new technologies are increasingly frequent in connection with the development of information technologies. This is true, e.g., of technologies providing for access to special-regime workplaces, mostly based on fingerprint scanning or iris recognition. Where fingerprints are transformed into a unilaterally encrypted binary string of numbers that cannot be used to reproduce the fingerprint, this does not

constitute processing of sensitive biometric data. The Office registered processing performed by a company engaged in the development of hardware and software in the area of identification of persons based on fingerprint recognition. The employees' fingerprints are processed with a view to keeping and processing a database of fingerprints for the purposes of testing the technologies and programmes being developed. For the purposes of these technologies, it is necessary to verify how the fingerprint will change over the year depending on the season and whether or not anomalies will occur in identifying persons at different temperatures and under other physiological influences. The processing takes place with consent of the employee being tested. Another interesting case registered by the Office involves processing notified by a bank in respect of signature as biometric data – specifically data concerning its size and dynamics, pressure in writing the signature and the time required for writing the signature – with a view to securing and enforcing legal claims in cases where there are doubts or disputes as to the authenticity of a signature. The two latter cases indeed involved processing of sensitive biometric data.

Frequent mistakes are made in respect of processing biometric data in the use of anthropometric characteristics (weight, height, age, sex, size of clothing, etc.). However, in those cases where the said individual anthropometric data are used in isolation, these are not biometric data as they do not allow for direct identification or authentication of the data subject as required by the Personal Data Protection Act. These data are processed especially by casting and modeling agencies with a view to establishing databases of hostesses and fashion models, and companies engaged in the area of nutrition and diet consultancy, as well as dating agencies, which process these data in relation to their activities.

The development of information technologies is also reflected in the ways in which employees are or can be monitored at their workplaces. Along with classical means, such as camera surveillance systems, this also involves increasingly sophisticated instruments that are capable of monitoring employee's work. These are, for example, software systems operating on a similar principle as, for example, antispam software. They are based on automated control of keywords.

Protection of confidential information is most frequently declared as the purpose of data processing. The personal data are processed by means of automated unspecific control of employees' business electronic communications based on keywords. This processing might involve uncertainty as to the possible duty to register such processing with the Office. The answer will always depend on specification of the individual purposes of processing. If the purpose of the processing lies in protection of business secrets in the sense of Article 17 of the Commercial Code, it can be stated that such processing is necessary for compliance with the controller's legal duty and thus subject to the exemption from the registration duty pursuant to Article 18 (1) (b) of the Personal Data Protection Act. However, the processing must always take place only within the scope required to attain the said purpose.

Similar to the previous year, the Office registered several entities performing research in the areas of medicine and genealogy. The data must always be processed with consent of the data subject.

Mention must also be made of notified instances of processing that indicate a certain trend in the area of commercial provision of health care. It is purely up to the client which equipment he orders, e.g. a blood pressure gauge, glucose meter, pedometer, etc. The controller processes the data exclusively on the basis of the client's explicit consent.

Similar to the previous year, data processing in camera surveillance systems was the most frequent type of processing (approx. 42 %). A total of 8621 entities that have made notification of personal data processing through camera surveillance systems are entered in the register of personal data processing. Notification was made by 1886 entities in 2012, which is a 25.3 % increase compared to 2011. For this reason, in co-operation with other departments, the Registration Department prepared and the Office issued a brochure titled “Operation of camera surveillance systems – Methodology for complying with the basic duties imposed by the Personal Data Protection Act”, which should facilitate the preparation of deployment and operation of camera surveillance systems by entities operating such systems (i.e. controllers or processors). The methodology is available to interested parties in both printed and electronic form and has also been translated into English.

■ TRANSFER OF PERSONAL DATA ABROAD

The long-term trend of decreasing numbers of applications for authorisation of transfers of personal data abroad ended in 2012. In 2012, the Office received a total of 17 applications for authorisation of transfer of personal data to third countries and issued a total of 18 decisions (compared to only 8 in the previous year). Geographically, this involved mostly transfers to the United States of America, Turkey, India and countries of Southeast Asia and the Pacific (South Korea, Malaysia, Hong Kong, Australia), and more frequently also to Eastern Europe (Russia, Ukraine). Of the said 18 decisions, the Office discontinued the proceedings in one case as the applicant had withdrawn his application; in four cases, the Office set the application aside, either because the applicant had ultimately resolved to provide for the anticipated data transfer through an agreement with the data importer including standard contractual clauses as its integral part or because the applicant limited the transfer only to countries of the European Union, or had entirely abandoned the intention. In the remaining 13 cases, the Office authorised the transfer.

In two cases, an authorisation was issued on the basis of Article 27 (3) (b) of the Personal Data Protection Act, because the applicant had established sufficient guarantees of personal data protection in the given third country. In one of these two cases, sufficient special guarantees were established through an agreement between the controller (exporter) and the processor (importer) in India. Based on the ascertained facts, and particularly based on the wording of the agreement on personal data processing executed between the controller and the processor, the Office was able to conclude that the agreement on personal data processing would establish sufficient special guarantees of personal data protection in the third country and that Article 27 (3) (b) of the Personal Data Protection Act would be fulfilled in the transfer of the personal data. In the other case, the applicant proved the establishment of special guarantees for the transfer of personal data within a multinational corporation to which the applicant belonged by submitting the Binding Corporate Rules of the group, which had been approved by a data protection authority in the EU as the “lead Data Protection Authority” within a special approval procedure the requisites and course of which were defined by Working Party 29 in working papers WP 74, WP 107, WP 108, WP 133, WP 153, WP 154

and WP 155. In addition to this case, two other entities attempted to apply for transfer of personal data within a group of companies based on binding corporate rules and the Office also answered several inquiries that indicated that the inquiring parties were preparing themselves for lodging an application for approval, but required clarification of certain issues: These were especially the questions of by whom the application was to be lodged, in what language it was to be drafted, whether and in what languages attachments should be enclosed, including especially the binding corporate rules of the group, and what other requirements had to be fulfilled in respect of the application.

Within its decision-making related to authorisation of transfers, in 2012 the Office discussed applications for authorisation of transfer of personal data of airline passengers to Ukraine. The Office came to the same conclusion as in similar previous cases of transfer of personal data of air passengers to Kuwait and Cuba. In its decision, the Office took account of the fact that the party to the proceedings intended to transfer personal data of its passengers only through the APIS system, and thus only to a limited extent involving personal data that are de facto given in passports and air tickets, rather than through its booking and check-in systems as is the case in transfers of data from the records of passenger names (PNR data). In the decision, the Office also took into account Article 13 of the Convention on International Civil Aviation of 7 December 1944, (Chicago Convention), published under No. 147/1947 Coll., under which the carrier must comply with the laws and regulations of a contracting State as to the admission of passengers to or departure thereof from its territory.

In relation to the transfers of personal data, the Office increasingly often deals with the issue of provision of cloud services by providers established outside the EU and EEA.

It is necessary to distinguish two main actors in data processing using a cloud system: the user and the cloud provider. According to the opinion of WP29 of 1 July 2012 dealing with cloud computing (WP 196), in all types of basic clouds (IaaS, PaaS, SaaS), the provider of cloud services is in the position of processor. If the data stored in the cloud leave the territory of the Czech Republic (i.e. to third countries not providing adequate level of protection), this constitutes their transfer in the sense of Article 27 of the Personal Data Protection Act. In these cases, it is necessary that the controller himself accept responsibility for safe transfer of data and legalise such transfer by utilising one of the instruments ensuring appropriate protection of the data being transferred, such as standard contractual clauses or BCR. In relation to the provision of cloud services, WP29's opinion of 6 June 2012 (WP 195) established another instrument for safe transfers of personal data to third countries – BCR for processors.

Legislative activities

The Office **considered the Government's programme of fighting corruption and ensuring transparency of decision-making of the public administration**, which was accompanied by a number of legislative and other measures, the most important comprehensive agenda in 2012, involving a number of issues related to stipulating proper statutory rules for the treatment of information, including processing of personal data.

The Office referred to foreign experience that the objectives of transparency (of public administration) cannot automatically outweigh the right of individuals to protection of their personal data.

The overall quality of legislative drafts in the Czech Republic in terms of the rules of treatment of information, operation of information systems and personal data processing was not satisfactory. The shortcomings were related particularly to shortened deadlines for drafting legislative materials, deadlines for commentary procedures, "non-standard" and inconclusive resolution of comments and also lacking substantiation of new instances of data processing proposed in the laws.

For the said reason, the Office appreciated that before the end of the year, the Government adopted modified legislative rules with a new **duty to evaluate the impact of individual draft laws on the protection of privacy and personal data**, not only in drafting substantive intentions of laws, but also of explanatory memoranda.

In the area of electronic communications, in 2012 the Office welcomed the Government draft amendment to the Electronic Communications Act, the Code of Criminal Procedure and some other laws, which was concerned exclusively with **maintenance and utilisation of traffic and location data for electronic communications**. Traffic and location data are newly defined in the Electronic Communications Act on the basis of the informative value of the individual data. As a rule, the recipient of an electronic communications service whose identity is known to the court or prosecuting body will be subsequently informed ex officio of any order for determination of these data.

The **area of public administration information systems and basic registers** was an area in which the Office lacked fundamental necessary changes in the protection of personal data in 2012. A reason for this state of affairs may lie in the progress of work in implementation of basic registers and links to the individual “sectoral” public administration information systems. The individual results of this work and related analyses may indicate certain shortcomings, particularly duplicate systems or data in public administration, or inappropriate combination of data. The Office pointed out that once public administration information systems are interconnected and purpose-based provision of data is systematically arranged, it might be more tempting to misuse the commonly utilised statutory authorisation, which was originally introduced in the system of records of the population, specifically that of all the “provided data, the competent authorities may use, in a certain case, only such data that are necessary for fulfilling the given task”.

Relations to foreign countries and international co-operation

In relation to the legislative proposal for comprehensive reform of personal data protection in the EU, the Office as the central administrative institution in the area of personal data protection drew up, in co-operation with the affected ministries, a draft framework position of the Czech Republic on the GDPR proposal for negotiations in the working bodies of the EU Council, which also served as an opinion for the Parliament (both the Chamber of Deputies and the Senate). In this position and also in the subsequent procedures, the Office dealt critically particularly with the following issues: modernised principles of personal data processing; further specification of the nature and form of consent to processing; (re)defining the basic notions, such as the relationship of sensitive data and high-risk processing; reconsideration of the roles of the entities responsible for personal data processing (controller and processor); clearer regulation of processing of personal data of youth and selected authorisations related to special personal data processing for law enforcement purposes. In view of all the comments and suggestions, the Office asked itself particularly whether the proposed wording of the new European rules for personal data protection, that is aimed at broadly regulating everyday conduct of individuals, entrepreneurs and institutions, was formulated in precise terms, comprehensibly and purposefully so as to meet the requirements on a *regulation* - i.e. a piece of legislation that is directly applicable and basically equivalent to a law.

In the decision on **accepting the responsibility** for negotiating the draft general regulation on personal data protection, account was taken of the opinion of the Ministry of the Interior of the Czech Republic and some other ministries that it would not be suitable to entrust the Office with responsibility for the preparation of European regulations, because the Office is an independent administrative authority – i.e. not part of the Government and not bound by its instructions. Subsequently, in the position of one of few authorities actively commenting on the draft legislation, the Office provided its opinions on the draft instructions for the individual stages of negotiations.

Through its representative, the Office also took part in negotiations at plenary meetings and at meetings of the committee of the Council of Europe T-PD group, where the Office's employee performs the duties of vice-chair and has contributed to commenting on and finalising the **proposal for modernisation of Convention No. 108**.

The topic on which the Office focused, and not only in relation to the preparation of the new legal framework for personal data protection, was **cross-border enforcement of the right to protection of personal data**. The OECD expert group discussed the Best Practices and the draft individual methodologies for global co-operation among several supervisory authorities both in Europe and overseas. WP29 dealt with practical findings from supervision over non-European personal data controllers, particularly those that operate popular web portals and services.

While the findings from countries in which these controllers are established or where they operate data storage facilities demonstrate that the requirements for personal data protection have been formally fulfilled, at the same time, these findings reveal problems related to compliance with all the principles and the necessary guarantees for personal data protection unless the requirements ensuing from European law are already taken into account in the design of the web applications (typically, Facebook). In view of this fact, in 2012 the Office supported, in WP29, those decisions that granted authorisation to selected national supervisory authorities to assess recent changes in the terms of personal data protection adopted by selected providers of web services (e.g. Google and Microsoft).

In 2012 the **Office was again involved in projects** of support for supervisory authorities in countries applying for accession to the European Union. Four employees of the Office accepted the invitation to present expert papers at workshops intended for their colleagues in partner institutions, particularly in Macedonia, Albania and Moldova. The most popular topics included the aspects of personal data protection in the fields of finance and police and also performance of supervision, communication with the public and international transfers of data.

Furthermore, the Office received funds from the Lifelong Learning programme/Leonardo da Vinci – Partnership in implementation of the **international project of "Raising Awareness of Data Protection among Employees Working in the EU"**. This project follows on from the successful co-operation in the past years when the Office took part, within the same programme, in a project that examined the topic of data protection from the viewpoint of employers.

In 2012 the Office also provided its statements on the aspects of personal data processing in two fundamental political and legal issues with an international element:

In respect of **introduction of the information duty of financial institutions required by the tax administration of the United States of America** under the Foreign Account Tax Compliance Act (hereinafter "FATCA"), the Office pointed out the need for clarifying the legal grounds for determining, gathering and further operations with data of persons with "American indications" and the need for the relevant legislative changes without which the said practices would be in contradiction with the Personal Data Protection Act. At the same time, the Office became involved in discussions concerning the legal regulation of transferring personal data gathered within the **FATCA** agenda by financial institutions or the tax administration in the Czech Republic to the United States of America under the conditions stipulated by Article 27 of the Personal Data Protection Act.

Negotiations on the Anti-Counterfeiting Trade Agreement among the European Union and its Member States, Australia, Canada, Japan, Republic of Korea, United Mexican States,

the Kingdom of Morocco, New Zealand, Republic of Singapore, the Swiss Confederation and the U.S.A. (“**ACTA**”) revealed shortcomings in the traditional approaches to law enforcement in the complex environment of the Internet. No detailed arrangements were incorporated in ACTA that would explicitly refer to the standards governing personal data protection in the European Union and its Member States. However, there was no doubt that personal data would be processed under the Agreement. The Office therefore considered the draft provisions of the Agreement related to processing of information (and thus also personal data) unclear and unbalanced in terms of the principles of personal data protection, as the draft wording of ACTA did not stipulate the level and corresponding instruments for personal data protection that should be applied. In its opinion sent to the Ministry of Industry and Trade and the related negotiations, the Office pointed out that to a major extent, the ACTA trade agreement was based on personal data processing in the area of new technologies (internet) and extended to several specifically regulated areas, such as confidentiality of communications, processing of traffic and location data, disclosure of communication for specific law enforcement purposes, processing of large quantities of data concerning not only parties to bilateral legal relationships, but also third parties (both suppliers – providers of services and electronic communication networks, and providers of information society services, their employees, parties and service recipients).

In the draft wording of **ACTA**, the Office considered especially flawed those instruments that promoted collection of information on third parties outside the purpose of law enforcement in courts. The Office pointed out that the purposes of enforcement could not be used to set new data flows and order disclosure of information (often processed originally for other purposes), without it being simultaneously defined in what manner the information should be transferred and disclosed. The Office thus recommended to reconsider the wider framework of the relevant legal regulations.

Work in **expert committees of the WP29 working party for data protection**, an advisory body of the European Commission, of which the Office is a member and its President vice-chairman, resulted in publication of four documents concerned with personal data processing with the use of new technologies in 2012. These documents included opinions on face recognition in on-line and mobile services, on development biometric technologies, on exemptions from the requirement for consent to cookies and on the topic that was discussed most by the professional public in the past year – **cloud computing**.

The Office, media and means of communication

In 2012 the Office again organised a press conference on the occasion of the Personal Data Protection Day. As usual, the conference served as an opportunity to announce another edition of the competition for children and youth “My Privacy! Don’t look, don’t poke about!” (for more details, see below). At the press conference, the Office also presented the journalists with an overview of its activities in the past half year. The second regular press conference took place in the second half of the year.

Record-breaking 90 media outputs on personal data protection were published in the two days following the January press conference – the daily number of serious media news concerning personal data protection varies, on average, between 5 to 9 articles.

The following topical subjects were particularly followed by the media in 2012: the ACTA anti-counterfeiting agreement; Google Street View; PNR data (transfer of airline passenger data between the U.S.A. and the European Union); portal znamylekar.cz; publication of data on debtors; cameras installed in means of public transport; personal data and IZIP; publication of photographs of alleged thieves; publication of salaries of public officers – Methodology issued by the Ministry of the Interior and the Office in this area; photo traps; monitoring of postmen with the use of GPS; amounts of fines imposed in relation to unsolicited commercial communications; a fine imposed on the Ministry of Education, Youth and Sports for publishing personal data of Roma scholarship beneficiaries; leak of photographs from a police file; monitoring at workplaces; camera surveillance system at the Superior State Attorney’s Office in Prague; personal data thefts; approval of a German law permitting sale of personal data by “cities” to private companies; monitoring the nationality of tourists in the Czech Republic with the use of mobile telephones; issue of the police DNA database; ski passes; and publication of recordings from meetings of municipal assemblies.

Within dissemination of knowledge of personal data protection (which is among important tasks of data protection authorities in all countries where such an institution has been established), in 2012 the Office focused on an increasingly pressing issue – the use of the internet by young people – and asked them whether they were really aware of the consequences of accessing this popular means of communication. The partners of the competition in 2012 included Czech Radio Prague, International Film Festival for Children and Youth in Zlín (where the prizes were handed out to winners) and also the Association of Library and Information Professionals (SKIP), which has available a list of contacts for libraries throughout the Czech

Republic, which are very active in working with children and youth, as had already been confirmed by mutual co-operation in 2012.

The Office provides detailed information on the results of the competition in a special section of its website.

In 2012 the employees of the Office again participated in a number of professional lectures and conferences. There were a total of 31 such events and some of them were specially adapted, based on agreement with the organiser, to the circle of participants (e.g. exclusively employees of the organiser); others were more general in nature or were specialised according to the discussed aspects (municipalities, electronic information, activities of the police in personal data processing, data security, etc.). Special attention was paid in 2012 to dissemination of information on the Office's competence related to the operation of basic registers.

The Office organised the third edition of the annual conference titled Security and Personal Data Protection, where the professional public and representatives of the Office had already twice met and discussed news in this area in terms of the conditions of personal data protection.

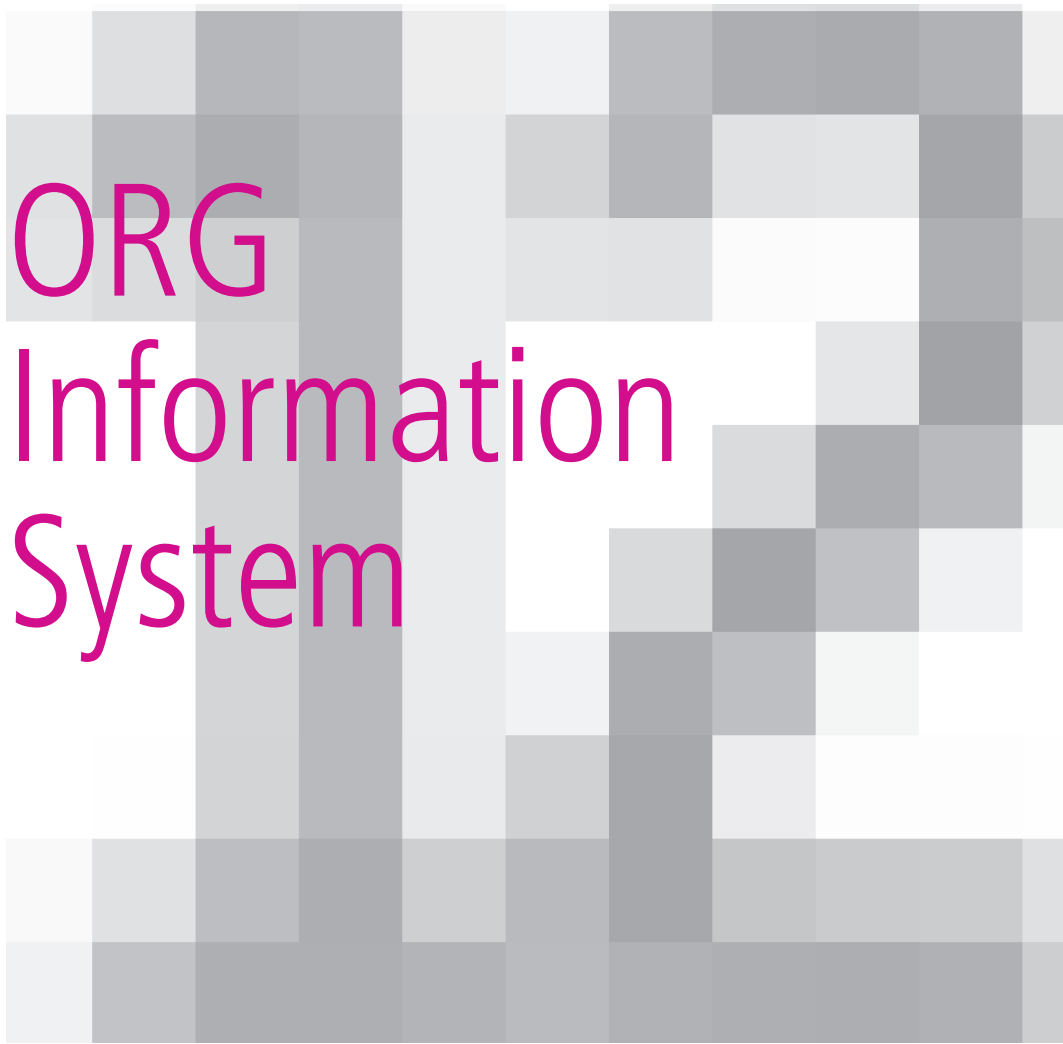
A new form of communication with the professional public were round tables organised on various topics in 2012.

In January 2012, on the occasion of the Personal Data Protection Day (28 January), the Office organised a round table concerned with the topic of media approach to personal data protection. Another round table arranged by the Office together with the ORSEC company was held in October and focused on camera surveillance systems. At the end of 2012, in co-operation with the Kinstellar law office, the Office held a round table concerned with the legal aspects of monitoring employees, also in the context of criminal liability of legal persons. The conditions for transfer of personal data abroad were another topic of this meeting.

The library provides a professional background for employees of the Office. However, it is also open to professional public on request. It is used by students for their seminary papers and diploma theses concerning personal data protection. In 2012 it provided its facilities to three students and obtained one diploma thesis prepared with the use of its contents. The library was extended by 78 publications - 64 were purchased and 14 donated to it.

In 2012 the Office published volumes 61 to 63 of its Journal. The positions published by the Office in the Journal are intended for professional workplaces and governmental institutions and also include important foreign documents dedicated to personal data protection. A volume of the Information Bulletin focused on the subject of basic registers was issued in 2012.

At its press conference held in the autumn of 2012, the Office informed the participants that it would create a new website which would be innovated not only in visual terms, but particularly in terms of user comfort and improved search options. Work on the system began after the Office checked the opinions and needs of the users of the website by means of a discussion forum.



ORG Information System

The “ORG Information System in the System of Basic Registers” was completed and launched in 2012.

The objective of incorporating the ORG Information System in the system of basic registers is to protect the citizens’ identity against misuse of their personal data. ORG is the only instrument that can transfer agenda indicators from one agenda to another.

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.



Project of “Optimisation of Processes of the Office”

The Office completed the second year of implementing the project titled “Optimisation of the Processes of the Office”, which is aimed at increasing the quality and effectiveness of the internal processes and setting the project management system. The Office thus follows the aims of the “Smart Administration” Government strategy, which aims at improving public administration services with the use of money from the structural funds. The project is financially supported from the European Social Fund within the Operational Programme “Human Resources and Employment”, specifically from the priority axis “Public Administration and Public Services (Convergence)” and area of support “Reinforcing Institutional Capacities and Effectiveness of Public Administration”.

The project will continue in 2013, when all the approved changes will be gradually implemented in the operation of the Office.



Personnel of the Office

The State budget established 102 functional positions in the Office, where this number did not change compared to the previous year. The age structure of employees remained the same as the year before. The structure of education also remains almost identical as in the past year; most employees of the Office have university education (62.89 %), compared to 62.6 % the year before. This high percentage is related to the requirement of the Office for university education, particularly in the areas of law and IT, for a majority of positions.

The interest of students and graduates of secondary schools and universities in obtaining professional practice or internship at the Office is growing every year.

Economic management of the Office

The budget of the Office was approved by Act No. 455/2011 Coll., on the State budget of the Czech Republic for 2012.

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

	in CZK thousand
Summary indicators	
Total income	89,566
Total expenditures	203,555.71
Specific indicators – income	
Total non-tax and capital income and accepted transfers of which: total income from the budget of the European Union. excl. SZP	89,566
other non-tax and capital income and accepted transfers in total	84,991.88
	4,574.12
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	44,292.01
Mandatory insurance premiums paid by the employer*)	15,624.07
Contribution to the Cultural and Social Needs Fund	424.76
Salaries of employees within an employment relationship	34,335.36
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	104,626.45
of which: from the state budget	15,657.92
contribution from the EU budget	88,968.52
Total expenditures recorded in the information system of programme financing	110,695.59

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

INCOME

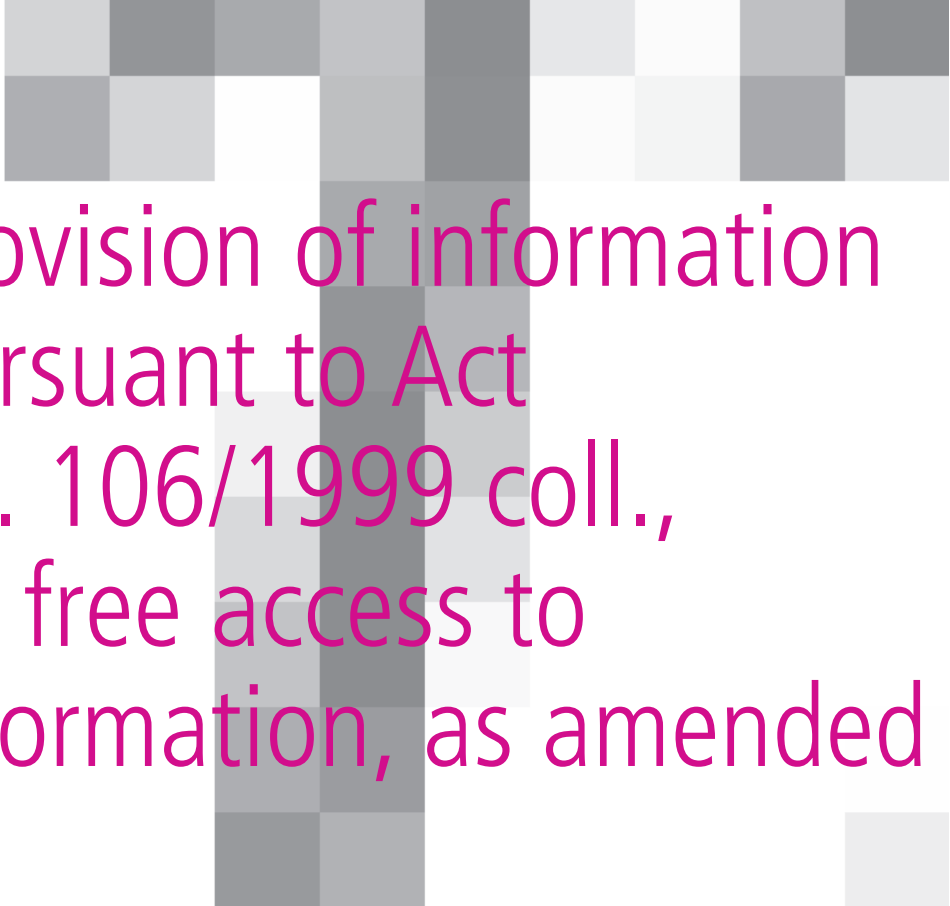
The income for 2012 was set by the approved budget at CZK 22,942 thousand in relation to the projects co-financed from the EU budget – IOP “ORG Information System in the System of Basic Registers” and the project in OP “Human Resources and Employment” titled “Optimisation of Management Processes of the Office”.

The total income of Chapter 343 – Office for Personal Data Protection equalled CZK 89,566 thousand.

This included, in particular, a refund for foreign trips by employees of the Office from Europol and the European Commission; penalties imposed pursuant to Act No. 480/2004 Coll., on certain services of the information society; penalties imposed pursuant to Act No. 101/2000 Coll., on personal data protection, and other laws; reimbursement of the costs of proceedings; interest accrued on funds deposited in bank accounts; refund of expenditures related to the EU Leonardo da Vinci Programme “Raising Awareness of Data Protection among Employees Working in the EU”; refund of expenditures for the project of Technical Assistance to Macedonia; income related to 2011 (remitting the balance of the deposit account after the payment of salaries and contribution to the FSCN for December 2011).

Interest on money deposited in accounts kept by the Czech National Bank equalled CZK 0.24 thousand.

Punitive payments received in the amount of CZK 3,775.78 thousand; investment and non-investment EU subsidies in the amount of CZK 84,991.88 thousand; insurance indemnities in the amount of CZK 36.44 thousand; non-capital contributions and compensations received in respect of previous years, including transfers from other funds of the Office in the amount of CZK 761.66 thousand. All income of the Office was transferred to the State budget.



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

In 2012 the Office received a total of forty-two requests for information pursuant to the Free Access to Information Act. Compared to the previous year, this number almost doubled. Of the total number of requests for information, in 2012 the Office fully satisfied twenty-nine requests, partly rejected ten requests and fully rejected three requests. The most frequent reason for rejection or partial rejection of a request for information lay in personal data protection. The Office also rejected a request for information on the grounds of protection of third-party business secrets, for reason of protection of confidential information and, in one case, also because the applicant requested information not available to the Office which the Office is not obliged to have at its disposal.

In a total of eight cases, the decisions on partial or full rejection of the request for information were contested by an appeal; the appellate body, i.e. the President of the Office, accepted the appeal in two cases. The procedure of the Office in dealing with requests for information was twice contested by a complaint pursuant to Article 16a of the Free Access to Information Act. The reason lay in the fact that the applicant had not been provided with all the requested information and a decision on rejection of a request for information had not been issued in respect of information that had not been provided. In one of these cases, the shortcoming was remedied by the first instance body, which provided the requested information to the full extent through the procedure pursuant to Article 16a (5) of the Act, and in the other, the decision on the complaint was made by the President of the Office, who satisfied the request and provided the information himself.

In most cases, the applicants requested information concerning the supervisory activities of the Office, such as a certain administrative decision or inspection finding, or a decision or statement of the Office concerning a certain area of personal data processing. Another major group of requests for information comprised requests concerning the economic management of the Office.



Annual Report Summary 2012

The Office for Personal Data Protection

Pplk. Sochora 27, 170 00 Praha 7

E-mail: posta@uouu.cz

Web: www.uouu.cz

In February 2013, 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.