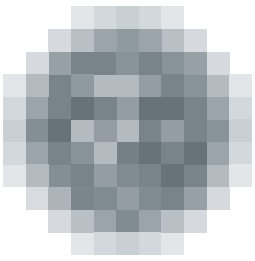
Annual Report Summary 2013



úřad pro ochranu osobních údajů
the office for personal data protection

The President of the Office Looks Back at 2013

During the year, the Office observed that, in addition to the persistent personal data protection problems experienced by the responsible entities when processing large amounts of data, some truly old problems, long thought to be resolved, were reappearing. Inspections that took place in accordance with the 2013 inspection plan identified issues related to processing of large amounts of data. Based on these issues – issues that are both old and new – we were forced again after many years to bear witness to the incomprehensible efforts to crucify debtors and evade valid legal regulations.

In connection with the information gathered, I have great hopes that the possible impacts on privacy will be considered when new laws are being drafted, which, as I mentioned in last year's annual report, will help prevent situations where the possible difficulties with personal data protection are only discovered after a regulation is adopted.

Nevertheless, new judicial rulings are also a very valuable source of information for applying the supervisory duties of the Office for Personal Data Protection – and a part of this annual report focuses on this source explicitly.

In 2013, the Office exercised its authority granted to it in 2012 to deal with "data breaches", i.e., monitoring and prosecuting breaches of electronic communication, and although it offered a comfortable reporting procedure

for the entities with reporting obligations – an electronic form facilitating mandatory reporting to the Office – I have to say that this area is definitely not one where the Office is most active.

In connection with the scandal where citizens of the European Union and politicians of European governments were being monitored by the National Security Agency (NSA) of the United States, the Office is cooperating fully with the European Commission within its structures. The Office has also been active in the case of Google's failure to provide sufficient personal data protection; specifically, the Office helped to create a group under Working Party 29 to investigate the matter, and this investigation has led to a number of countries imposing harsh fines on this company.

We continue to believe that the newly amended European personal data processing legislation will help clear up a number of complicated cases, some of which I have mentioned, although it is becoming apparent that the new EU personal data protection regulation is not taking form easily, just as work on harmonising the modernised Convention 108 of the Council of Europe is far from over. The Office is actively taking part in consultation procedure now underway in respect of the drafted regulation, the sponsor of which in the Czech Republic is the Ministry of the Interior. 2014 is set to become a turning point for personal data protection in Europe: We are anticipating that even comments on the Safe Harbour mechanism, which regulates the transfer of personal information between Europe and the USA, will be resolved once the 13 requirements presented to the United States by EU Justice Commissioner Reding for improving personal data protection are satisfied.

As in previous years, we placed emphasis on educating youth and holding discussions with experts: the round tables organised by the Office continue to be a well-established form of consultation (amongst the other consultation obligations of the Office).

Not even in 2013 did the Office abandon its practice of maintaining active international contacts. It used these connections to consult certain issues with or worked with them directly (as an example I can mention the Leonardo programme, where we are working with our Polish, Croatian and Bulgarian counterparts). It is only natural that in addition to day-to-day obligations (the Office received 7428 communications requiring attention over the course of the year!), the Office is involved in an "international personal data protection network", as only in this way can positive progress in personal data protection – that is privacy and the freedom of each and every individual in a functioning democracy to make decisions – take place.

Igor Němec

CONTENTS

THE OFFICE IN NUMBERS 2013

Inquiries and consultations	inquiries in the Czech Republic	2994
	abroad	15
	consultations	3013
	for state administration	126
	for local governments	195
	for legal persons	532
	for natural persons operating a business	298
	for natural persons	1863
	of the total number of consultations	
	in person	235
	in writing	2778
Requests and complaints	instigations received pursuant to Act No. 101/2000 Coll.	1336
	complaints referred to inspection of administrative procedure	139
Unsolicited commercial communications (competence pursuant to Act No. 480/2004 Coll.)	total instigations	7428
	instigations resolved	5463
	inspections initiated	90
	inspections completed	91
	administrative decisions on a fine	33
	challenged by objections	8
	objections accepted	1
	objections dismissed	5
	mostly accepted	0
	mostly dismissed	1
Inspections (excluding inspections concerning Act No. 480/2004 Coll.)	initiated	90
	completed	74
	referred to other governmental authorities	0
	challenged by objections	15
	objections accepted	1
	objections dismissed	11
	mostly accepted	3
	mostly dismissed	4
	analyses	11

Administrative punishment	adminsitrative proceedings for violation of Act No. 101/2000 Coll. and Act No. 133/2000 Coll.	101
	infraction proceedings pursuant to Act No.101/2000 Coll.	18
	administrative and infraction proceedings pursuant to Act No.13 101/2000 Coll. – Article 44 a, 45 a	13
	infraction proceedings for violation of Act No. 159/2006 Coll., on conflict of interests	0
	appeal decisions on violation of law	32
	appeals dismissed	23
	cancelled and returned to new hearing	3
	cancelled decisions and proceedings discontinued	2
	change in the decision	3
Judicial review *NB: * in total since 2001)*	court actions lodged	18 (118*)
	actions dismissed by the court	8
	decisions cancelled by the court	3
	court proceedings closed/pending since 2001	74/44
Registration	notifications received (pursuant to Article 16 of Act No.	6570
	processing operations registered	5994
	still pending	867
	registrations cancelled	97
	notifications on a change in the processing	878
	proceedings pursuant to Article 17	85
	discontinued (no violation)	71
	discontinued for procedural reasons (e.g., notifications withdrawn)	19
	not permitted	7
Authorisations for transfers of personal data abroad	applications for transfers of personal data abroad (pursuant to Article 27 of Act No. 101/2000 Coll.)	25
	decisions on authorisations of transfers	20
	decisions on dismissal	0
	proceedings discontinued for procedural reasons	4
Notifications pursuant to Act No.127/2005 Coll.	notifications received	1
	notifications found justified	0
	notifications found unjustified	1
Complaints pursuant to Article 175 of the Code of	complaints received	40
	complaints found justified	10
	complaints found partly justified	7
	complaints found unjustified	24

Applications pursuant to Act No. 106/1999 Coll.	applications received	79
	fully accepted	47
	partially accepted	22
	applications rejected	10
Materials published	Office Journal (number of volumes)	3
	Information Bulletin (number of volumes)	1
Press conferences	regular	2
	ordinary	0
Legislative drafts on which comments were made	laws	69
	implementing regulations	95
	draft government regulations	17
	draft decrees	78
	other	60
	foreign materials	25

SUPERVISORY ACTIVITIES OF THE OFFICE

• 2013 INSPECTION PLAN

I. GENERAL TOPICS FOR SPECIFICATION OF SUPERVISORY ACTIVITIES OF THE OFFICE´S INSPECTORS IN 2013

1. INFORMATION SYSTEMS WITH LARGE AMOUNTS OF DATE

Unlike previous years, where the inspectors' supervisory activities were divided up to focus on information systems either in public administration or on those in the private sphere, the main content of the 2013 plan was monitoring the scope of various information systems in terms of the amount of processed data in relation to the number of data subjects and in relation to the number of subjects involved in the entire processing process.

This approach is in response to continuing efforts to interconnect systems despite their being originally created for certain and predetermined purposes; it is, therefore, necessary to observe in what way processing is taking place and how the rules for determining the responsibility of various entities are set up.

Such systems are created not only in the banking and insurance industries, but also in the social system, including the provision of welfare and social services. At the same time, the development of services known as "personal assistance services", where data about the state of health of a patient is linked to data about his or her other personal needs, has to observe the rights of each individual to be informed in advance about the scope of processing.

The ever more pervasive application of technology, where the tendency is to promote the electronic processing of databases only, for example for the purposes of keeping medical records (currently according to Act No. 372/2011 Coll., on health services and the terms and conditions for the providing of such services) is closely tied to this issue.

In the area of information systems, the following inspections were conducted:

a. Observance of the data controllers' obligations under Act No. 101/2000 Coll., on personal data protection ("Act No. 101/2000 Coll."), where the

inspection was focused on the processing of personal data of natural persons in connection with the **operation of teller and dispatch systems operated at ski resorts**.

b. Observance of the controllers' obligations under Act No. 101/2000 Coll. in connection with the **processing of personal data of power company customers**, with focus on the fulfilment of the conrollers' obligations under Article 5(4) and Article 11 of Act No. 101/2000 Coll.

c. Observance of obligations in connection with the **operation of a hospital information system** – protection of the patient privacy, security of electronic medical records.

d. **Processing of customer data** pursuant to Act No. 101/2000 Coll. **in connection with offering bank services** (customer awareness, personal data security, scope of information provided to clients).

e. Processing of personal data of eligible persons in connection with the provision of **foster care benefits** (Act No. 359/1999 Coll., on the social and legal protection of children).

Inspection of the processing of personal data of customers pursuant to Act No. 101/2000 Coll., in connection with an **offer of fitness centre services** (operation of a camera surveillance system, customer cards).

2. OTHER ITEMS IN THE 2013 INSPECTION PLAN

In connection with the latest findings and experience from past supervisory activities, the Office focused on the following:

a) Processing of the personal data of participants in training courses falling under projects and programmes in the area of state employment policy (Act No. 435/2004 Coll., on employment).

b) Preparedness of the Czech Republic on the transition to SIS II.

c) Observance of the obligation of responsible entities in connection with reporting the results of criminal proceedings to the trade licencing offices and accessing criminal records [Article 6(4) of Act No. 455/1991 Coll., the Trade Licence Act].

d) Observance of the obligations under Act No. 101/2000 Coll. in connection with procedures related to processing and declassifying information on aid applicants and recipients in terms of the application of Act No. 171/2012 Coll., by which Act No. 218/2000 Coll., on budgetary rules, is amended.

e) Conditions for processing customer data in the area of offers of goods and services, not only in the framework of Act No. 10/2000 Coll., but also in other areas in the remit of the Office related to certain information society services in accordance with Act No. 480/2004 Coll., on certain information society services.

f) Observance of personal data protection in the processing of Schengen visas.

g) Processing of personal data by responsible entities pursuant to Act No. 101/200 Coll., in connection with handling complaints.

Specifically the following inspections were conducted:

1. Observance of obligations pursuant to Act No. 101/2000 Coll. in connection with the processing and disclosure of personal data about aid applicants and beneficiaries under the **State Agricultural Intervention Fund**.

2. Observance of obligations pursuant Act No. 101/2000 Coll. in connection with the processing and disclosure of personal data about aid applicants and beneficiaries under the **State Housing Development Fund**.

3. Processing of personal data by the responsible entity pursuant to Act No. 101/2000 Coll. in connection with the complaints handling in the remit of the **Czech Medical Chamber**.

4. **Processing of personal data of retraining participants** in connection with projects and programmes in the area of state employment policy (Act No. 435/2004 Coll., on employment).

5. Observance of the obligations of the responsible entity in connection with the processing of personal data by the **operator of the on-line discount portal** www.skrz.cz.

6. Observance of personal data protection in the **Schengen visa processing procedure** by the consular departments of Czech embassies. Investigations at the consular departments of the Czech embassies in Kiev, Rabat and Belgrade. Investigations that were performed pursuant the Office´s inspection plan were based on the recommendations of a committee of experts for the Schengen assessment of member states in the area of personal data protection.

7. Investigation of the degree to which the Czech Republic is ready for the **transition to SIS II**. The investigation focused on the degree to which the Police of the Czech Republic is able to ensure the security of personal data processed in the national part of the Schengen Information System in connection with the migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information system (SIS II).

8. Observance of the obligations of responsible entities in connection with reporting the results of criminal proceedings to the **trade licencing offices** and accessing criminal records.

II. INSPECTIONS FROM THE 2012 INSPECTION PLAN COMPLETED IN 2013

1. In the period from September 2012 to January 2013, an inspection of the "on-line shop" operated by **Internet Mall**, a.s. was conducted. The inspection was aimed at the processing of personal data of customers/clients making purchases through the website www.mall.cz.

2. In 2013, an **inspection at the Ministry of Transport** was completed from the 2012 inspection plan. This inspection, conducted from September 2012 to February 2013, focused on personal data processing in connection with operation of the central vehicle register (the "CVR").

3. The **inspection at the Ministry of Labour and Social Affairs**, as the responsible entity for operating the Single Information System of Labour and Social Affairs, commenced in March 2012 and was completed in 2013. The inspection was aimed at observance of obligations set out in Act No. 101/2000 Coll., specifically the security of personal data in the Single Information System of Labour and Social Affairs.

4. The inspection at **CERD ČR,** s.r.o., which also commenced in 2012, was, with regard to the large number of complaints that the Office obtained from dissatisfied individuals, moved to 2013.

III. INSPECTIONS STARTED IN 2013 INITIATED BY THE PRESIDENT

In connection with publicly disclosed information and an instigation delivered to the Office on 23 July 2013 regarding access to the internal system of **Penzijní společnost Komerční banky** through the Internet banking system of Komerční banka and the presentation of the entire procedure via a publicly accessible video recording, reasonable concerns were raised as to whether the actions of the entities responsible for processing personal data in connection with the operation of the internal system of Penzijní společnost Komerční banky did not in fact result in a breach of the obligations of the controller or processor under Act No. 101/2000 Coll.

• FINDINGS OBTAINED BY INSPECTORS IN INSPECTION ACTIVITIES

In 2013, inspectors of the Office carried out 74 incidental inspections on top of inspections under the inspection plan. As is the case every year, many complaints concerned the processing of personal data of data subjects via recordings from camera surveillance systems, especially those located in residential buildings. Inspections were conducted with respect to camera surveillance systems located at workplaces, the processing of personal data by a health insurance company in connection with the statutory possibility to register with a different health insurance company, personal data processing in debtor databases and security of information systems.

CZECH MEDICAL CHAMBER

Based on the 2013 inspection plan of the Office, an inspector initiated an inspection at the Czech Medical Chamber (the "CMC"), the subject of which was a review of the observance of the data controller's obligations under Act No. 101/2000 Coll. in connection with handling a complaint regarding the professional performance of its members pursuant to Article 2(2)(e) of Act No. 220/1991 Coll., on the Czech Medical Chamber, Czech Dental Chamber and the Czech Pharmacists' Chamber, with a focus on the activities of the regional association ("RO") of CMC Děčín, expanded to include a review of the activities of the RO of CMC Most.

The inspection did not confirm any breach of Act No. 101/2000 Coll., on personal data protection.

INSPECTION OF ZNANYLEKARZ SP. Z.O.O., THE COMPANY OPERATING THE WEBSITE WWW.ZNAMYLEKAR.CZ

The subject of the inspection was observance of the data controller' obligations under Act No. 101/2000 Coll., with a focus on the processing of data subject's personal data published on the website www.znamylekar.cz operated by ZnanyLekarz Sp. z.o.o. (the "Company"), with its registered office in Poland.

The Company, by making personal data pertaining to specific individuals carrying out their activities in the Czech Republic available in the Czech Republic, is involved in processing personal data in the Czech Republic. The Office for Personal Data protection of the Czech Republic is the locally pertinent authority to perform supervision over personal data processing that takes place in the Czech Republic. Czech physicians and other medical workers (the "medical workers") began turning to the Office with complaints that the Company was publishing their personal data on the website www.znamylekar.cz, both in the "Basic profile" of medical workers and particularly in the section "Opinions and information" (discussion forum) without their consent. They further stated that the Company did not respond to their requests for removal of their personal data. Based on these complaints, the Office initiated an inspection of the Company.

During the inspection, it was found that the Company is the website operator and, thus, the controller of the data published on the mentioned website and that the servers on which the

data are stored are located in France. The personal data of medical workers can be posted on the website by any user who registers with the Company; such registered user can also enter comments and evaluations regarding the work of a specific medical worker in the "Opinion and information" section (discussion forum).

A medical worker can also register with the Company and create his or her own verified profile. Without registering, however, he or she cannot respond in any way to the comments made by users in respect of his or her profile, although the website operator guarantees this in its terms and conditions.

The appointed inspector performed a legal assessment of the processing of personal data of medical workers on the website www.znamylekar.cz and based her assessment on the documents that the Company published on its own website about personal data processing rules.

By processing (publishing) personal data about medical workers in the "Basic profile" section of www.znamyleakr.cz, the Company is not in violation of Act No. 101/2000 Coll., as such personal data may be processed (published) without the respective individuals' consent based on an exception under Article 5(2)(d) of Act No. 101/2000 Coll., as the personal data is obtained by the Company from public sources, i.e., namely from the database of physicians published on the website of the Institute of Health Information and Statistics of the Czech Republic. The personal data of medical workers published in the section "Opinions and information" (discussion forum), with respect to which the Company does not have a valid registration, are data published by the Company without their consent, i.e., at variance with Article 5(2) of Act No. 101/2000 Coll.

According to the findings obtained by the inspector, in four specific cases, medical workers registered with the Company and their personal data on www.znamylekar.cz are published in the "Verified profile" section. These medical workers, by registering, granted their consent to the company to process their personal data on www.znamylekar.cz, i.e., the agreed to the terms and conditions set out in the documents issued by the Company. Subsequently, however, all four revoked in writing their consent to the processing of their personal data and submitted their decisions in writing to the Company and, in compliance with the Company's terms and conditions, requested that their records be removed from the database. The declared non-agreement with the publication of their personal data, including the request to remove any records from the database, is considered a revocation of consent with the processing of personal data, and ZnanyLekarz Sp. z.o.o. is obliged to remove such data not only in compliance with the law, but also according to its own terms and conditions.

The appointed inspector also observed that if the Company, as the provider of electronic services, learns about the unlawful nature of any stored information, it is obliged to address the situation immediately, as this obligation is stipulated in Article 5(1)(b) of Act No. 480/2004 Coll., on certain information society services. Specifically, it has to take any and all measures to remove or block information of an unlawful nature. In any case, if the provider is warned in a credible manner about the possibility of unlawful information being stored on its website, it is at least obliged to block such information to all users and review its content and the objections against its publication. If its finds the objections to be justified or demonstrable, it is obliged to remove such information. The only exception where the operator is entitled to retain the information is the protection of its rights and its legally protected interests in resulting proceedings; in such case, however, the operator must always ensure that the

personal data are not available to the public. This means, for example, the retention of data for the needs of the law enforcement authorities should it be suspected that a crime was committed or in the case of a legal dispute regarding damage compensation etc.

If a medical worker is still interested in resolving the matter through the courts even after his or her personal data are removed, and thereby having the possibility to prove that the data published was entered by a different user and was of an unlawful nature and that by the publication of such data his or her personal rights were violated, the company is obliged to keep an exact record of data of registered individuals (users) so that it can provide such data to the user upon his or her request in the event of a civil law suit.

The appointed inspector also stipulated corrective measures to be adopted by the company: to refrain from processing personal data of medical workers on its website www.znamylekar.cz without their consent and to remove the personal data of medical workers published on www.znamylekar.cz (i.e., the personal data of medical workers who filed complaints with the Office and whose data are specified in the inspection protocol), with the deadline for doing so being without delay.

In the written response sent to the Office by the Company, the Company argued that the Polish Office for Personal Data Protection ("GIODO") had jurisdiction and that it found that the databases managed by the Company are reported to it and that the inspection conducted by it showed that the data managed by the Company are processed duly and in compliance with the law. According to the Company, the personal data were obtained from the Internet, where they are widely available. In the Company's opinion, it is not possible to territorially restrict media such as the Internet.

As the Office has the powers of a central administrative authority for personal data protection in the scope stipulated by Act No. 101/2000 Coll. in the Czech Republic, it does not have the possibility to exercise its powers and enforce corrective measures on an entity that falls under the jurisdiction of the Polish Republic and, thus, the scope of the inspection was limited.

The above-described steps taken by the Office for Personal Data Protection, including the initiation of an inspection of a company that is headquartered abroad but, as a data controller, processes personal data in the Czech Republic, are without precedent. It is specifically for this reason that the objective of the Office is to present this issue and, if possible, enforce the protection of personal data of data subjects (in this case, Czech physicians), whose personal data on the Company's website www.znamylekar.cz in the "Opinion and information" section (discussion forum) are processed without consent, i.e., at variance with Czech law. A review of this case by European data protectors may help find a solution to one unresolved issue (known as "one-stop shop"), which is being discussed as part of the European regulation being drafted to replace Regulation 95/46/EC.

The above steps being taken by the Office, however, do not preclude the possibility of the Czech physicians whose data are being processed on www.znamylekar.cz without their consent turning to the Czech courts with a civil law suit on the protection of personality and demand that the Company not only remove their personal data from the website but also compensate them.

The Office continues to defend the following opinion published on 15 July 2013 on www.uoou.cz in the column Supervisory activities/Control activities of inspectors: The issue of enforcing one's rights to the protection of private and family life should a website operator

argue freedom of speech and the right to publish the opinions of third parties, and where, at the same time, the operator and author hide behind the anonymity of the Internet, is complicated but not impossible to resolve.

INSPECTION AT A HEALTH INSURANCE COMPANY

An inspection of a health insurance company (the "HIC") was initiated based on an instigation sent to the Office by the Czech Police, which received a report against a person suspected of committing an offence under Article 44(2)(e) of Act No. 101/2000 Coll., when in November 2011, such person, as the data processor, processed the complainant's personal data without her consent and drew up an HIC Application and Personal File, thereby re-registering the complainant from the General Health Insurance Company of the Czech Republic to a different insurance company without her knowledge.

The appointed inspector initiated an inspection at the HIC in June 2013, the subject of which was a review of the observance of the obligations of a personal data processor under Act No. 101/2000 Coll., with a focus on the processing of personal data of individuals insured by the HIC in connection with their registration.

The appointed inspector assessed the mentioned personal data processing and found that the unauthorised registration of the complainant with the HIC and thus the unauthorised processing of personal data by the HIC had really occurred.

The inspection showed that the HIC did not have such mechanisms in place that would, in case that re-registration of insured individuals does not take place via personal contact with an employee at branch of the insurance company, i.e., in a way that allows for the proper verification of the identity of the applicant, indicate that a "fictitious" Application and Personal File were submitted. The HIC did not have in place any control mechanisms set up with respect to the company with which it had concluded a processing agreement that would allow it, as the processor of personal data of clients (insured parties) and potential clients, to collect and process such data in compliance with Act No. 101/2000 Coll.

Furthermore, the appointed inspector stated that the agreement that the HIC concluded with the company that arranged the re-registration of clients contained only the HIC's declaration that it transfer responsibility to the processor but no guarantee from the processor that the personal data is technically and organisationally secure. The HIC thus failed to fulfil its obligations as a personal data processor under Article 6 of Act No. 101/2000 Coll., as without verifying what technical and organisation security its data processor has adopted, at variance with its obligations under the law, transferred its responsibility to a different person. The purpose of Article 6 of Act No. 101/2000 Coll. is to prevent the data controller from relieving itself of its responsibility to secure protection of personal data.

CAMERA SURVEILLANCE SYSTEMS AT WORKPLACE

The subject of the inspection that the appointed inspector initiated on the premises of the investiateded company (the "investigated party"), which is involved in locksmithery and toolmaking, was observance of the obligations under Act No. 101/2000 Coll. related to personal data processing via a camera surveillance system with recording equipment, operated on the premises of the controlled party. The "representatives" of the employees of the controlled party sent an instigation for an inspection to the Office in which they called attention to the breach

of employee privacy at the controlled party due to the use of a camera surveillance system installed at the workplace and stated that the objective of the monitoring system was not to improve safety and security at the workplace, but only to place pressure on the employees (telephone calls "Where were you?" - "In the restroom", etc.) and to instil fear in existing and new employees. At the same time, the initiators of the instigation called attention to the fact that the workplaces of the controlled party are not categorised as high-risk work places. In this connection, they referred to the Charter of Fundamental Rights and Freedoms, Act No. 101/2000 Coll., Act No. 40/1964 Coll., the Civil Code, and Article 316(2) of Act No. 262/2009 Coll., the Labour Code. They further stated that the images from the camera surveillance system were watched by certain individuals directly at the company but also from private premises.

The inspection found that the case concerns industrial production on the grounds of the controlled party that is entirely fenced in and comprises a number of buildings. The investigated party employs close to 80 people who work predominantly in the investigated party's own production in three-shifts (non-stop operations). The subject of the investigated party's business is machine production, predominantly small-batch production, which in practice means that certain employees need not necessary work continuously (during a shift) on one machine, and their workstation may change depending on technological procedures when work is being done on a certain product or depending on immediate production requirements. Except for minor exceptions, production is not automated, so employees work on a number of machines during the production process. In addition to operating their own respective machines, the employees may or must move about in the area around the machines, for example from the material storeroom (semi-finished products), back to their machines and then to the storeroom to store completed parts. Should the machines be misused or material stored in the workshops go missing, it is not possible with regard to the above-described technological procedure to determine a specific party as the perpetrator.

In light of the above, the investigated party decided to install and operate a camera surveillance system based on previous negative experience with theft and unauthorised use of machines by employees.

As the investigated party carries out surveillance as prevention against the unauthorised use of its machines and technical equipment and to safeguard material, and the recordings made should be used exclusively for the purpose of clarifying any transgressions, with the employees being informed by their employer about such surveillance in advance, such surveillance is not a breach of the employees' privacy. The appointed inspector assessed the situation as one where the aforementioned processing of data is not a violation of Article 5(2)(e) of Act No. 101/2000 Coll., on personal data protection.

It was further discovered, however, that the investigated party, in connection with the operation of the camera surveillance system with recording equipment, breached the information obligation of a data controller [under Article 11(1) of Act No. 101/2000 Coll.], as it did not inform the data subjects of their right to access their own personal data or about their other rights stipulated by Article 21 of Act No. 101/2000 Coll., nor did it inform third parties via information signs who the data controller is.

In connection with inspection findings, the investigated party was instructed as follows to remedy the situation: To fulfil the information obligation under Article 11(1) of Act

No. 101/2000 Coll. and provide additional information about who processes the persons data via the camera surveillance system and for what purpose; and to amend internal regulations, specifically to inform data subjects about the right to access personal data, about the right to correct personal data, as well as about other rights set out in Article 21 of Act No. 101/2000 Coll., on personal data protection.

CAMERA SURVEILLANCE SYSTEM AT A PLACE OF RESIDENCE AND ON THE PREMISES OF A CAR REPAIR SERVICE

Based on an instigation for an inspection of the observance of obligations imposed on data controllers under Act No. 101/2000 Coll., the appointed inspector commenced an inspection at the premises of the investigated company (the "investigated party") focused on the processing of personal data using a camera surveillance system with recording equipment operated in two locations: on the premises of a residential building and on commercial premises, specifically a car repair shop. According to the complainant, the first camera surveillance system was installed at the investigated party's residential address for the purpose of monitor the entrance to a restaurant operated by the investigated party's former wife. The reason for the installation of the camera installation system was to protect the private property (vehicles) belonging to the i nvestigated party. The second camera surveillance system was, according to the complainant, installed on the front of the premises of a car repair shop. In the complaint, the complainant states that the investigated party shows the recordings taken by the camera surveillance system to his friends and checks the movement of individuals around the mentioned restaurant.

The appointed inspector discovered during an on-site inspection that the eight cameras are installed on the premises of the car repair shop, of which seven were in operation at the time of the inspection. The camera system was operated continuously, with the recording being activated by a motion sensor in the field of vision of the camera, and the cameras recorded in colour and had infrared lighting for night vision. The digital video-recorder kept recordings for 14 days, after which the recordings were automatically recorded over. The recording equipment was stored in an open credenza located in the investigated party's office. The recording equipment was connected to a monitor that displayed the current view of the cameras in ordinary on-line regime. Only the investigated party had access to the office; other people had access only if accompanied by him (e.g., the investigated party's son, who sometime helped repair vehicles). Access to the recording in the recording equipment was possible based on a user name and password that only the investigated party created and knew.

No guidelines or similar documents related to the operation and security of the camera surveillance system were drawn up by the investigated party, as no one else but he had access to the equipment.

The reason for the installation of the camera surveillance system was multiple break-ins and property damage, specifically vandalism, of which the investigated party suspected the complainant of perpetrating. Since the installation of the camera surveillance system, no further instances of vandalism occurred; for this reason, the investigated party did not hand over the recordings made by the camera surveillance system to anyone else. By viewing the camera urveillance system recordings and during the on-line transmission, the inspection discovered that the quality of the image is sufficient to identify the recorded individuals.

The inspection also found that the investigated party did not speak the truth when he claimed that he leased the adjacent parking lot monitored by cameras nos. 1 and 2 from the municipality.

The appointed inspector, as part of the legal assessment, stated that despite the fact that the parking lot is used by significant number of the investigated party's clients, and the investigated party thus can argue that he is protecting his client's property, the mentioned parking lot is not reserved only for the investigated party's business operations. By keeping recordings made of the entire parking lot using the camera surveillance system, the investigated party violated his obligation as a data controller to process personal data only with the consent of the data subjects pursuant to Article 5(2) of Act No. 101/2000 Coll. Prior to completing the inspection, the investigated party rectified the situation. The appointed inspector imposed corrective measures to be taken by the investigated party: to supplement the registration with the Office within seven days of this inspection protocol becoming final, as he failed to arrange from the beginning of May 2013 to the inspection date of 6 August 2013 his reporting duty to the Office set out in Article 16(1) of Act No. 101/2000 Coll., by which he violated Article 16(1) of Act No. 101/2000 Coll., on personal data protection.

SKARTA (SOCIAL SYSTEM CARD)

According to the 2012 inspection plan of the Office, in November 2012, an inspection at the Ministry of Labour and Social Affairs (the "Ministry"), as the controller of the Single Information System of Labour and Social Affairs (the "SIS"), was commenced in November 2012 and completed in January 2013. The inspection was aimed at the processing of personal data of eligible persons and benefit recipients in connection with the issuance of the social system card.

The Office also obtained a number of instigations containing concerns about the suspected violation of Act No. 101/2000 Coll. for the reason of the unauthorised disclosure of data about eligible persons and benefit recipients to Česká spořitelna, a.s. ("ČS, a.s.").

As the Ministry was not authorised by a special act to disclose the personal data of eligible persons and benefit recipients to ČS, a.s. in connection with sKarta, the social system card [Article 4a and Article 4b of Act No. 73/2011 Coll.], the disclosure of personal data to ČS, a.s., being an unauthorised person, took place without any legal basis.

The Ministry thereby violated its own obligation in connection with securing personal data under Article 13(1) of Act No. 101/2000 Coll., i.e., to prevent unauthorised access to personal data.

The appointed inspector imposed on the Ministry the obligation to remedy the situation by the stipulated deadline.

INSPECTION OF OBSERVANCE OF THE OBLIGATIONS TIED TO THE SECURITY OF PERSONAL DATA IN THE SINGLE INFORMATION SYSTEM OF LABOUR AND SOCIAL AFFAIRS

The problems that arose in connection with the payment of non-insurance social benefits in January 2012 because of the transfer to the new benefit payment systems resulted in a lot of media coverage. The statement made by the information technology designers working at the Labour Offices about their concerns regarding the security of data contributed substantially to the uproar. The databases operated by the Ministry of Labour and Social Affairs (the "Ministry")

manage the economic, media and social data of more the half of the Czech population. From the point of view of Act No. 101/2000 Coll., such data is for the most part sensitive data. Immediately after the disclosure of the mentioned statement, the Office received seven instigations from both natural and legal persons, based on which it initiated an investigation in March 2012 at the data controller, which is the Ministry.

During the inspection, it was discovered that two people could access the system under one user name. The problem with the entire Single Information System (the "SIS") was that it operated from the very beginning without logging the access of authorised persons. In the period from January to February 2012, i.e., in the initial phase of operation, it even operated without each employee having his or her own individual access authorisation.

Once the inspection was completed, two remedial measures were imposed on the Ministry based on the inspection findings: to cancel with immediate effect the e-mail instruction asking employees to use a shared user name and to arrange for the supplier of the applications to ensure that all access to the SIS is logged.

EURODAC SYSTEM (ELECTRONIC DATABASE OF FINGERPRINTS OF ASYLUM SEEKERS)

The inspection stemmed from the 2013 inspection plan of the Office and was executed based on a recommendation of an expert committee for the assessment of the Member States in connection with personal data protection under the Schengen system.

The inspections focused chiefly on ascertaining in what way, if at all, the system administrator controls that the processed personal and sensitive data are kept up-to-date and accurate in accordance with Article 5(1)(c) of Act No. 101/2000 Coll. and on a review of security measures and personal data protection in accordance with Article 13 of the same act.

The fingerprints of asylum seekers older than 14 years of age are entered in the EURODAC system and are stored in the system for ten years; only in the event that the foreigner obtains citizenship of the respective state will the fingerprints be deleted from the system. Prior to the dactyloscopy being performed, the foreigner is informed in writing that he or she is entitled to have his or her data deleted from the EURODAC system if the data is sent to the system illegitimately; he or she is further informed that the request for deletion of incorrect data be sent to the Office directly. The appointed inspector checked ten records randomly chosen according to registration numbers to see whether the controlled data were stored legitimately in the EURODAC system. The EURODAC system also contains the fingerprints of every foreigner detained in connection with illegal entry into the country; in the Czech Republic this only happens at airports as this country does not border any countries that are not in the European Union.

The appointed inspector did not discover any violation of Act No. 101/2000 Coll.; in relation to the above legislation, the Ministry was, however, recommended to work with the General Administration Department of the Ministry, specifically its State Citizenship and Vital Statistics Office, in the event a foreigner receives Czech citizenship. This office is responsible for granting Czech citizenship; in other words, this information may be sent without delay to the Ministry's Asylum and Migration Policy Office, which then requests the Criminology Institute of the Police of the Czech Republic to delete the Czech citizen's data from the EURODAC system. Should an applicant obtain the citizenship of a different EU Member State, the inspector

recommends taking international action to exchange such information, which is necessary for storing exact and complete information in the EURODAC system. At the end of the inspection protocol, the inspector recommended that the Ministry work with the Police Presidium of the Czech Republic to adopt internal supervision system regarding to authorisation to access the EURODAC system to ensure observance of the conditions of Article 13 of Act No. 101/2000 Coll. (logging).

OPERATION OF TELLER AND DISPATCH SYSTEMS AT SKI RESORTS

The control system checks children's tickets without any further processing of personal data, seasonal tickets issued in the name of a specific holder with further processing of personal data and other tickets without further processing personal data.

The Company processes its clients' personal data in the following extent: name, surname and photograph of the holders of season tickets while the tickets are valid and not longer than until the end of the ski season (approx. 4 to 5 months). The reasons for the stated duration of processing personal data are client claims, client complaints and the possibility of use of the tickets by unauthorised persons. The control system is technically set up so that it is possible to ascertain the unauthorised use of a seasonal ticket retroactively.

The inspection conclusion stated that the period of processing the photographs of ticket holders and other personal data is commensurate with the above-mentioned reasons.

The inspection found that clients of the Company are not informed in accordance with Article 11(1) of Act No. 101/2000 Coll., about the scope and purpose for which the personal data are processed or who the data controller is; information about the rights of data subjects under Article 21 of Act No. 101/2000 Coll. in connection with the processing of their personal data is also missing.

The inspection found that the company, as at the date of commencement of the inspection, did not inform the Office that it is processing personal data, thereby violating Article 16 of the Personal Data Protection Act.

These two violations of Act No. 101/2000 Coll. were resolved by the imposition of corrective measures on the inspected company in the various inspection protocols.

CENTRAL REGISTER OF DEBTORS – CERD

In 2013, the Office also focused on the operator of the CERD debtor database. The reason was not only the number of complaints and instigations, but also the interest shown by the public and the media.

The inspection found that the inspecteded party was only the processor – the data controller is headquartered in the USA. The appointed inspector stated that obligations connection to personal data processing under Article 5(1)(d) and Article 21(1) of Act No. 101/2000 Coll. were breached. In compliance with Article 40(1) of Act No. 101/2000 Coll., after taking into account the inspection findings, the inspected entity was imposed corrective measures, including the obligation to inform the Office of their fulfilment.

At the same time, the inspection protocol contained recommendations for the inspected entity to improve the comprehensibility of the services offered and to avoid further complaints

addressed to the Office. The complaints chiefly concerned the publication of false or incomplete and inaccurate personal data. Communication with the above processor is also poor: Data subjects are unable to arrange for the deletion of illegitimately processed or inaccurate personal data.

With regard to the fact that the Office is assigned certain powers under the law for processing personal data in the Czech Republic and in places where Czech laws can be enforced under international law and European standards of personal data protection can be guaranteed, the Office has no possibility of exercising its powers on or demand corrective measures from an entity falling under the jurisdiction of the USA and, thus, the inspection could only be conducted to a limited degree.

KB PENZIJNÍ SPOLEČNOST, A.S.

In mid-20013, the media reported on a leak of personal data from the database operated by Komerční banka, a.s. (the leak did not concern personal data from a database run by Komerční bank, a.s. but from a database run by KB Penzijní společnost, a.s.).

The inspection discovered a breach of the obligations under Article 13(1) of Act No. 101/2000 Coll. As the investigated party stated already at the time of the inspection that it had added control mechanisms to the defective application that ensure proper user authorisation in a way that prevents the generation of a defective link, thereby ensuring verification of access to the website in the application, no corrective measures were imposed.

The case is a flagrant example of the risk of modern communication based on use of the Internet. This was not a hacker attack on the security system of the bank – this was an error in an application that should have prevented unauthorised access to the system. The investigated entity did not discover an error during control tests and the system could have continued operating in this way for a much longer time if a client had not informed the bank of the problem.

The inspection found that the data controller failed to sufficiently secure the stored personal data. The software that should have protected the data contained an error and allowed the leak of information.

With regard to the above, the appointed inspector stated that he considers the obligation on the part of the data controller to perform an internal risk assessment to be a justifiable request.

PURE HEALTH & FITNESS, S.R.O.

The inspection found that many of the obligations under Article 5(1)(d) and (e) and (2), Article 11(1) and (2), Article 13(1), (3) and (4), Article 16(1) and Article 20(1) of Act No. 101/2000 Coll. were breached. Ten corrective measures were imposed on the investigated party, including the following obligations: to modify the paper version of Pure Club membership application form; to amend the *Guidelines for processing personal data for PURE club members*; and to modify the technical and organisational measures concerning the retention of records from the camera surveillance system or improve the way clients are informed about the installation of the camera surveillance system in the fitness rooms. The inspection findings showed that the fitness operator highly underestimated the issue of privacy protection. With regard to the number of clients of the investigated company, this was a relatively serious finding.

An overall assessment of the case, however, also shows carelessness on the part of the data subjects, as they provided even non-mandatory data without any effort to find out the purpose

for which this data is to be processed. For this reason, the Office plans to focus on this issue in the next period as well.

VIDEO RECORDINGS FROM MEETINGS OF A MUNICIPAL COUNCIL VIA THE MUNICIPALITY WEBSITE

In connection with an on-site inspection at, and discussions with, the investigated party, it was discovered that the municipal council, through a resolution, approved a Statement of Purpose stating, among other things, that the municipal council has decided to open the town hall to the people or, more precisely, that the town hall will promote efforts to make the town as open as possible to its citizens. In respect of this, an agreement between the investigated party and a private television broadcaster on the production and broadcasting of the television and Internet programme "U nás ve městě" ("Here in our town") was concluded; the agreement contains the terms and conditions of exercising the rights to the programme and to make recordings of the meetings of the municipal council and exercising the rights to such recordings, as well as the terms and condition of the production and broadcasting of the television and Internet programme "Městský express" ("Town Express").

The appointed inspector concluded that the investigated party violated Article 6 of Act No. 101/2000 Coll., as the agreement concluded with the private television broadcaster did not contain the particulars required by Act No. 101/2000 Coll., specifically guarantees of the technical and organisational protection of personal data.

In the period from September 2011 to June 2013, the investigated party provided data subjects with information about the processing of their personal data. Missing from the mentioned notification, however, was information about the scope of the personal data processing, information about the purpose for which the personal data will be processed, who will process the personal data and how, and to whom the personal data will be available. Also missing was information about access to personal data, about the right to have personal data corrected and on the other rights set out in Article 21 of Act No. 101/2000 Coll. This situation changed at the municipal council meeting in June 2013, where the person chairing the meeting duly informed all those present at the meeting to the extent required by Article 11(1) of Act No. 101/2000 Coll. The investigated party had breached the information obligation ensuing from Article 11(1) of Act No. 101/2000 Coll. in the period from September 2011 and June 2013.

The investigated party breached its information obligation under Article 13(2) of Act No. 101/2000 Coll. because it, as the data controller, had not drawn up or documented the technical and organisational measures that would guarantee protection of the personal data contained in the video-recordings of the municipal council meetings.

The investigated party, in cooperation with the Office, managed to amend all agreements and internal documents to be in compliance with the Personal Data Protection Act practically just before the inspection protocol was issued, which in the case of local governments is exceptional.

• COMPLAINTS HANDLING AND PROVISION OF CONSULTATIONS

After years of ever increasing number of complaints and instigations, 2013 saw a levelling off. The relatively high number is a testament to the fact that people have become accustomed to enforcing their rights to privacy, which includes personal data processing, via the Office. The consultation activities of the Office are also contributing to the growing awareness of personal data protection.

Statistical data on complaints addressed in 2013

Total	1336
of which:	
referred for inspection	81
referred for initiation of proceedings	58
forwarded to the competent bodies	21
dismissed as unfounded	1176

As in previous years, the complaints pertained to a great extent on the degree to which camera surveillance systems were operated. This pertained in particular to camera surveillance systems operated in residential buildings.

2013 also saw a slight increase in complaints and instigations in the area of information technologies. This increase began in previous years in connection with the increase in the number of users of social networks and the Internet generally. Internet users are already aware that they leave a digital footprint when using the Internet, especially when using social networks on which they share their user content, including photographs, and are losing control over the dissemination of information about themselves.

The issue of negative registers, e.g., of debtors or persons with financial or property obligations, is another significant area of complaint in 2013.

Complaints and instigations made by the public concerning demands for copies of personal identity cards are frequent, as are complaints concerning the disclosure of personal data by municipalities.

Among the most frequent violations of the Personal Data Protection Act by data controllers or processors is the processing of personal data without legal purpose, their processing for a purpose that is different than the one they were collected for (this is also a frequent problem of local governments), and failure to adopt adequate measures to secure personal data in accordance with Article 13 of the Personal Data Protection Act. Failure to provide data subjects with information or explanations concerning the processing of their personal data despite written requests for such information or explanations is one of the most common transgressions. In the experience of the Office, the right to an explanation under Article 21 of the Personal Data Protection Act is especially underestimated by both data controllers and processors.

In 2013, as in previous years, the Office provided consultations. Personal data protection issues can be consulted even in person at the Office itself upon request; this opportunity is used by the public, institutions and big companies.

In 2013, the most frequent queries pertained to the operation of camera surveillance systems, handling of birth numbers, authentication of employees upon their being hired, records of working hours, transfers of personal data abroad, publication of personal data on the Internet and sending commercial messages.

A new trend appeared in 2013: the establishment of internal anti-corruption telephone lines. Unlike other countries, the Czech Republic does not have a special legal regulation concerning whistle-blowing. The Office organised a round table about the issue of whistle-blowing in terms of personal data protection, and this round table was attended by multinational companies providing services tied to whistle-blowing.

The Office also recommended to the Czech Trade Inspection the method it should use to disclose the final imposition of penalties so that such disclosure, from the point of view of personal data processing, does not infringe on the privacy rights of self-employed persons, as opposed to the original plan of the Czech Trade Inspection of blanket disclosure. In the second case, the functionality of the Central Vehicle Registry was examined.

• FINDINGS OBTAINED IN ADMINISTRATIVE PROCEEDINGS

PUBLICATION OF PERSONAL DATA OF DEBTORS

The Office considers the publication of personal data in connection with receivables (debt) to be an impermissible infringement on the privacy of individuals, as the disclosure of such data, obtained based on a private law relationship, can result in damage to the good name of such person in other private law and public law relationships.

The law provides sufficient means to protect a creditor's rights in those cases where specific debts on the part of customers/client are not paid, which includes enforcement of court decisions; the publication of lists of debtors is not one of these means, however. In practice, however, this topic was put on the back-burner in the first years of operation of the Office. It appeared that this practice was not very widespread among private law entities and that standard instruments provided by the law to creditors were being used to enforce receivables.

In 2013, a number of cases appeared (especially in connection with the operation of on-line shops) that could be an indication that creditors are reverting to this practice. Whether there is an actual reason (e.g., an increase in the number of debtors, greater difficulty in enforcing receivables through the courts, etc.) why this is happening is not too clear. It is, however, important to call attention to the unlawfulness of such practice and to warn those people planning to take such action against doing so.

When conducting administrative proceedings and, upon their conclusion, determining fines, the Office, in compliance with Article 46(2) of Act No. 101/2000 Coll., takes into account the severity, method, duration and consequences of the unlawful action as well as the circumstances under which it was committed. In practice, cases of publication of the personal data of debtors are assessed in terms of the number of persons affected by such action, the extent of the data disclosed, how long the data were in the public domain, whether any defamatory language (such as thief) was used in connection with the disclosure, and even the amount of the debt (in terms of the circumstances under which the offence was committed, the disclosure of debt in the hundreds of crowns should be assessed as more serious than disclosure of debt in the hundreds of thousands of crowns). In terms of method of publication, publication via the Internet to an unlimited group of people is clearly most serious, but other methods can be considered (the Office has, for example, encountered a case where dozens of posters were put up in the location where an alleged debtor lived).

Finally, it should be stressed that the imposition of fines in administrative proceedings does not mean that it is then possible to leave the personal data published on the public website with the argument that the data controller had already been punished for such disclosure. In such case, the administrative offence is deemed to be ongoing.

PUBLICATION OF INFORMATION ABOUT PERSONS SUSPECTED OF COMMITTING AN OFFENCE

A very contentious topic in terms of the public occurred in 2013 when a municipality published the personal data of individuals suspected of committing an offence on its website. A specific type of blacklist was created as a result.

In the inspection, the Office first stated that there are no legal regulations that would address the disclosure of personal data of individuals suspected of committing offences being dealt with by municipalities; therefore, the general provisions on personal data processing contained in the Personal Data Protection Act apply.

The claim that this approach is an effort to make the activities of the municipality more transparent is not acceptable, as municipalities are obliged even in connection with the publication of information on enforcement of the public funds for which it is responsible to observe all legal regulations, including the Personal Data Protection Act.

It should also be added that the publication of personal data on the Internet results in the creation of electronic footprints that link to the data subject, and these are difficult if not impossible to eradicate entirely. Furthermore, information published on the Internet can be accessed by an unlimited number of people, and so the dissemination of such information is quick and easy.

• FINDINGS FROM COURT REVIEWS

Numerous decisions of the Office are subject to court review. As regards specific findings from the relevant court rulings in 2013, it is possible to call attention to a number of important decisions regarding the operation of camera surveillance systems and the publication of personal data in particular.

SURVEILLANCE USING VIDEO CAMERAS, WHERE RECORDINGS ARE MADE AND THEN THE INDIVIDUALS WHO ARE RECORDED ARE IDENTIFIED IN THOSE CASES DETERMINED BY THE PERSONAL DATA ADMINISTRATION, IS DEEMED THE PROCESSING OF PERSONAL DATA, EVEN IN THOSE CASES WHERE THE RECORDED INDIVIDUALS ARE NOT IDENTIFIABLE IN PRACTICE

In the opinion of the Supreme Administrative Court, personal data is collected and processed even in situations where no additional information is provided with the only identifier, i.e., the face; nevertheless, it is possible to subsequently identify the person (from the date when a seminar or meeting took place, who organised it, the list of participants etc.). Furthermore, it can also be deduced that the purpose of the recording – protection of interests protected by law – assumes that such identification can be expected.

When it comes to camera surveillance of hotel premises, the Supreme Administrative Court expressly dismissed arguments referring to, for example, the high standard of the hotel or that the hotel provides the highest standard of services and that the legitimacy of the camera surveillance set up is derived from this. The Supreme Administrative Court, in the respective decision, declared its opinion that that a high level of services also includes a high standard of privacy protection of its recipients, i.e., the guests.

If protection of a human right or freedom is to be given precedence over protection of the right to privacy, then the situation must be one where fundamental human rights and freedoms, which are otherwise equal in standing, are in conflict and it is necessary to thoroughly consider whether in such situation the interest protected by a different basic right and freedom is so serious and under such a threat that it is possible to consider infringing on privacy, and thus partially or completely restrict the fundamental human right to privacy and private and family life, i.e., human dignity. If a camera surveillance system is to be allowed, as a means to achieve a certain end, which in the given case was to protect the safety and security of the persons and assets of the building owner and of the hotel guests and other visitors, it is necessary to assess in particular whether this camera surveillance system infringes on fundamental rights and freedoms, whether in the specific case the fundamental right or freedom protected by the camera surveillance system outweighs the protection of privacy, whether this means is the only and most appropriate one to protect the given interest or whether a different means is not available to achieve the given purpose, either without infringing on the fundamental right to privacy at all or to a lesser degree. At the same time, it is also necessary to assess the degree of proportionality, i.e., whether the infringement of the values by these means – in this case infringement of the right to privacy or human dignity and freedom – is commensurate, i.e., whether the

right to privacy deserves less protection than the value that should be protected, specifically the protection of the person or asset.

Camera surveillance can generally serve a number of purposes that can be grouped into a number of primary categories: 1) protection of individuals, 2) protection of property, 3) public interest, 4) detection, prevention and prosecution of crime, 5) collection of evidence, and 6) other legitimate interests. A key issue is, however, again the need to use such camera surveillance, i.e., whether it is not possible to protect rights and legally protected interests in some other way.

The respective ruling also addressed the conditions for the proper granting of implied, not express, consent by the data subjects. It mentioned that such consent may be possible, but only under the condition that this consent is given actively in a way that is not ambiguous; such consent must of course be able to be proven by the data controller, as it is the one that bears the burden of proof.

A LOCAL OR REGIONAL GOVERNMENT WITH AN ESTABLISHED POLICE FORCE IS NOT AUTHORISED TO SET UP A CAMERA SURVEILLANCE SYSTEM THAT WOULD LIKELY NOT BE PERMITTED IF IT WERE A PRIVATE ENTITY; IN THIS CONNECTION, IT CANNOT BE ARGUED THAT THE MUNICIPAL POLICE IS PART OF THE LOCAL OR REGIONAL GOVERNMENT IN QUESTION WHEN THE CAMERA SURVEILLANCE SYSTEM WAS IN FACT NOT INSTALLED FOR THE POLICE FORCE

According to the mentioned ruling, although the municipal police may not be an independent legal personality and the respective municipality is bound by the legal acts of the municipal police, it is necessary to call attention to the fact that in the assessed matter it is not decisive who has or does not have legal personality, but what the respective legal regime is and what purpose the camera surveillance system is in fact set up for. In the assessed matter, it was clear that not only did the police have access to the camera surveillance system, but that employees of the municipal office did as well. Therefore, if the camera surveillance was installed to maintain public order and protect life, health, property and other rights and legally protected interests, it should fully comply with Act No. 553/1991 Coll., on the municipal police; the camera surveillance system would then be managed only by the municipal police and only the municipal police would have access to it.

THE DISCLOSURE OF PERSONAL DATA OF THOSE PERSONS WHO CONTACTED THE MUNICIPALITY WITH THEIR INSTIGATIONS OR REQUESTS HAS TO BE BASED ON A LEGAL REASON THAT CANNOT BE DERIVED JUST FROM THE SPECIFIC ACT OF FILING

The Municipal Court in Prague ruled that the disclosure of personal data on the website of a municipality is not necessary for the handling of the requests, i.e., for fulfilling the purpose for which the personal data was collected. A request as such is not consent to disclosure of the personal data contained therein on the official bulletin board or website; it can only be understood as consent to process the personal data as part of request handling procedure.

The Municipal Court in Prague addressed the application of Article 8b(1) of Act No. 106/1999 Coll., on free access to information, according to which the obligor provides basic personal data about the person to who public resources were provided, with basic personal data meaning, in accordance with Article 8b(3) of Act No. 106/1999 Coll., name, surname, date of birth, municipality where the beneficiary has his or her permanent residence, and the purpose and conditions of the granted public resources. In the opinion of the Municipal Court in Prague, this provision is an exception to the general rule enshrined in Article 8a of Act No. 106/1999 Coll., according which information pertaining to personality, manifestation of fee will, privacy of a natural person and the personal data of the obligor shall only be provided in compliance with legal regulations governing the protection of such information. Thus, it is also necessary to proceed in compliance with the rules set out in Act No. 101/2000 Coll. even in connection with the disclosure of information according to Act No. 106/1999 Coll. As regards the application of the special regime under Article 8b of Act No. 106/1999 Coll., it was stressed that there is no obligation under this provision to actually disclose such information. Disclosure based on Article 5(3) of Act No. 106/1999 Coll. primarily requires the satisfaction of the respective request.

• REGISTRATION

In 2013, a total of 6570 notifications of personal data processing were submitted; thus the trend of a year-on-year increase continued. This year marked a 13% increase from the year before. The total number of requests from supplementation was 877 this year, which is slightly more than last year. In the second half of 2012, the Personal Data Processing Register was connected to the basic registers system and specific changes in addresses and identification data of the various subjects were reflected in it through the automatic updating of data from the basic registers. It is thus not necessary to make these changes through notification of changes in processing. In addition to the assessment of received registration notifications, the Office issues decisions on registration cancellation pursuant to Article 17a(2) of Act No. 101/2000 Coll. This year saw a total of 97 registration cancellations based on the request of data controllers, most often due to the winding up or merger of a company, cancellation of business activity or termination of personal data processing. Such cancellations grew 20% year-on-year. The Office published information about cancelled registration in the Bulletin.

As numerous personal data processing notifications did not contain the information that would allow sufficient assessment of the personal data processing or as the submitted documentation was not complete, the Office had to suspend the proceedings and send the notifying party a request to provide addition information pursuant to Article 16 of Act No. 101/2000 Coll. Of the 6570 notifications of personal data processing received, the proceedings related to 867 had to be suspended. In 63% of cases, the suspension pertained to notifications of processing using camera surveillance systems; in 11%, it pertained to the processing of sensitive data; in the remaining 26%, the suspension was due to other reasons.

In the event that the supplemented notifications led to concerns that the processing of personal data could result in a violation of Act No. 101/2000 Coll., administrative proceedings were commenced, which was the case with respect to 91 notifications (i.e., in 1.4% of notifications). Personal data processing was not permitted in the case of 8 notifications subjected to administrative proceedings pursuant to Article 17 of Act No. 101/2000 (i.e., 0.1% of the notifications).

When responding to requests, the staff of the registration department of the Office often encountered the issue of personal data processing in the framework of on-line shops, the possibilities for setting up cameras on certain premises, the necessity of consent with the personal data processing using a camera system, requests for assistance with filling in the notification of personal data processing, cancellation of the registered notification of personal data processing and requests for information of the status of the personal data processing notification. The subject of many questions and consultations pertained to the transfer of personal data abroad, especially within multinational corporations.

In 2013, the registration department, in cooperation with other departments of the Office, drew up the Methodology for the Fulfilment of Certain Obligations under the Personal Data Protection Act when Operating On-line Shops. This document should help entities operating on-line shops fulfil their obligations to the Office as well as other obligations stipulated by Act No. 101/2000 Coll. The document shall be available in electronic form on the Office's website.

In 2012, **Directive 2007/66/EC of the European Parliament and of the Council** was transposed by Act No. 468/2011 Coll., which amends Act No. 127/2005 Coll., on electronic communication. The regulation concerns, for example, the issue of the breach of security of personal data. In 2013, the Office obtained only one instigation regarding the breach of security of personal data, which, however, was filed by an entity to which this reporting duty does not pertain under this legislation.

It is apparent from the registration activity that there is a continuing tendency on the part of employers to monitor their employees at work through various available technologies. As part of the registration proceedings, the notifying parties are repeatedly warned that blanket monitoring and processing of the content of employee correspondence as part of e-mail processing are not allowed under Act No. 101/2000 Coll., nor are blanket monitoring and processing of the content of telephone calls. It is also necessary as part of registration proceedings to call attention to the risks tied to monitoring employees via geolocation devices.

A high percentage of processing notifications related to the use of loyalty cards. The purpose of the processing is generally the possibility to utilise certain discounts and benefits related to purchases made by the card holder, who states his or her name, address or other contact information if he or she is interested in receiving information about marketing events. The data controllers declare in the notifications that this occurs with the consent of the data subjects.

A relatively high number of notifications relate to whistle-blowing exclusively in connection with the Sorbanes-Oxley Act (SOX). Thus, the notifications only pertained to companies controlled by entities that are subject to this legislation and thus have the obligation to introduce a whistle-blowing system into their companies. Czech legislation does not contain any express provisions on whistle-blowing; only a draft of the "Whistle-blowing Act" exists. For this reason, the Office is dealing with the issue of personal data protection in connection with whistle-blowing only marginally. In 2013, the Law Faculty of Charles University organised an international conference on the topic of whistle-blowing, at which the Office also presented its contribution on this topic.

• TRANSFER OF PERSONAL DATA ABROAD

When observing the general principles of the lawful processing of personal data under Act No. 101/2000 Coll., data controllers may transfer personal data without the Office´s prior consent not only to EU Member States or countries in the European Economic Area, including Switzerland, but also to third countries with an adequate level of personal data protection. For it to be possible to transfer personal data to countries without adequate personal data protection, it is necessary to obtain authorisation from the Office in advance if such transfer is not regulated by an agreement that includes standard contractual clauses based on a decision by the European Commission.

In the authorisation proceedings, the Office reviews the specific circumstances of the transfer of the data from the Czech Republic to third countries, especially the source, scope and category of the transferred personal data, the recipient of the transferred personal data, including a list of the target countries, the purpose of the transfer and the processing period.

In the authorisation proceedings, the Office reviews the specific circumstances of the transfer of the data from the Czech Republic to third countries, especially the source, scope and category of the transferred personal data, the recipient of the transferred personal data, including a list of the target countries, the purpose of the transfer and the processing period. In addition to supplying the Czech version of the respective binding corporate rules (BCR) and the decision on their approval by the head of the supervisory body, it is therefore necessary to describe all circumstances in detail in the request.

In 2013, the Office accepted 24 requests for authorisation to transfer personal data to third countries. In all four cases, the Office suspended the matter for the reason that the applicant restricted the transfer to only EU Member State or to some other secure country.

Of the twenty authorisations issued this year, authorisations issued under Article 27(3)(b) of Act No. 101/2000 Coll. were the most prevalent for the first time ever, meaning applicants had established sufficient guarantees protecting personal data in the third countries through approved BCR. This was in the case of seven requests. In six cases, the authorisation was issued pursuant to Article 27(3)(a) of Act No. 101/2000 Coll., i.e., the transfer of data with the consent or based on the instructions of the data subjects. In five cases, the authorisation was issued based on Article 27(3)(e) of Act No. 101/2000 Coll., i.e., the transfer of data necessary for negotiations on concluding or amending an agreement at the request of the data subject or for the performance of an agreement to which the data subject is a party. The remaining two authorisations were issued based on Article 27(3)(c) of Act No. 101/2000 Coll., where the transfer concerned personal data that based on a special law are part of data files open to the public or open to those who demonstrate legal interest.

Geographically, the requests for authorisation involved mostly transfers of personal data to the United States of America, India, South-East Asia and the Pacific (South Korea, Japan, China, Hong Kong, Singapore), and in one case Kazakhstan. In cases where the transfers were based on BCR, personal data are, as a rule, transferred by making them accessible to branches of the group usually located in a greater number of countries or around the world.

In seven cases, the Office issued authorisation to transfer personal data based on BCR, specifically BCR-C (Binding Corporate Rules for Controllers). These are now labelled as classic

BCR that were and continue to be intended for multinational data controllers who, as part of their work, collect, transfer and process personal data across the multinational corporation for special purposes.

The approval procedure for these BCR-C on the part of any personal data protection authority in the EU, as the lead supervisory authority, continues to take place based on the mentioned documents of the Article 29 Data Protection Working Party (WP 29), specifically the documents published under the code WP 74, WP 107, WP 108, WP 133, WP 153, WP 154, and WP 155.

In addition to classic BCR-C, BCR-P (Binding Corporate Rules for Processors) have not been newly defined. These are intended for major multinational personal data processors, usually cloud service providers who process the personal data of a large number of data controllers. As in the case of classic BCR-C, BCR-P are also subject to approval by a data protection authority in the EU, as the lead supervisory authority, with this procedure, its particulars and course being defined in the Article 29 Data Protection Working Party in documents WP 195, WP 195a, and WP 204.

Just as in the case of BCR-C, it is also necessary in the case of BCR-P to request authorisation from the Czech Office to transfer personal data to a third country according to Article 27(4) of Act No. 101/2000 Coll. before such transfer takes place. The authorisation is not requested by the multinational processor, but by the various data controllers who have decided to use the processor's services, usually cloud services. It should be noted that a data controller who decided to process personal data in a multinational cloud is, in such case, responsible for the personal data processing and that the authorisation to transfer personal data to third countries has to be requested even in this case before commencing the transfer in compliance with Article 27(4) of Act No. 101/2000 Coll.

Doubts regarding the Safe Harbour programme, as an instrument for the secure transfer of personal data from the EU to the USA, is also shared by the Office; therefore, it continues to recommend to data controllers (data exporters) to verify before any transfer whether the certification of the respective company continues to be valid, whether and in what way natural persons are informed about the internal procedures for complaints handling, or whether the "privacy policies" of the respective company are publicly accessible through, for example, the website. The Office should be informed if any shortcomings are ascertained in connection with the application of the Safe Harbour principle.

In 2013, the Office, as part of its authorisation activities, also dealt with requests for authorisation of the transfer of Advance Passenger Information Data (API data) of airlines to the United Arab Emirate and to South Korea. As it had previously, the Office arrived at the conclusion that in the case at hand, the condition of Section 27(3)(e) of Act No. 101/2000 Coll. would be met, i.e., that the transfer will be necessary for the performance of an agreement to which the data subject is a party. 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 the departure of passengers from its territory. In this connection, the Office, in its decision, took account of the fact that airlines intend to transfer the personal data of its passengers 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 Passenger Name Record Data (PNR data). In 2013, the Office received a request for authorisation of PRN data to the Republic of Korean from an airline carrier. The Office has still not made a decision on the matter.

• SCHENGEN COOPERATION

In conformity with the Czech Republic's international cooperation obligations in the field of security, the Office effectively continued in line with established practice and in the exchange of information and experience regarding personal data protection.

In 2013, just as in previous years, the representatives of the Office took part in regular negotiations and efforts shared with supervisory bodies regarding supervision over extensive information systems, such as the Schengen Information System, the Visa Information System, Customs Information System and EURODAC, which processes chiefly the fingerprints of asylum seekers. In connection with the transfer to the second generation Schengen Information System, the operation of the European Council's Joint Supervisory Authority for SIS came to an end and was replaced by the SIS II Supervision Coordination Group, established under the European Data Protection Supervisor's Office, with the representative of the Czech Office attending the meeting of this group, which took place in the second half of 2013.

The Office again examined the security aspects of the migration to the new SIS II on the national level; this review, however, had still not been finalised by the end of 2013.

In 2013, the Office obtained 63 instigations regarding the visa policy of the Czech Republic, especially requests for information regarding visa proceedings, requests for meetings or other instigations, most of which were made in English, but also in Czech, French, Romanian, Russian etc., with the Office responding to all of them. It is of course necessary to state that visa applicants or people requesting related information erroneously believe that the Office has authority over visa policy in the Czech Republic. The Office, however, has authority in this area only if any of the extensive information systems operated in the Schengen area process personal data in an unauthorised manner.

In such case, the data subject, with regard to the fact that the principle of direct access to personal data is applied in the Czech Republic, is entitled to submit a request first to the information system administrator, which in the case of the SIS is the Police Presidium of the Czech Republic. If the Czech Police does not provide a data subject with a satisfactory response or does not respond at all within 60 days, the data subject is entitled to submit a complaint to the Office concerning the unauthorised processing of personal data, and only then can the Office exercise its supervisory powers. The respective forms and all information regarding the enforcement of the right to the protection of personal data in the area of Schengen cooperation are published on the website of the Office together with the respective request and complaint forms.

In 2013, the Office received a total of 9 requests regarding the processing of personal data in the SIS. With regard to the above, the requests were forwarded to the SIS administrator, i.e., the Police Presidium of the Czech Republic, for processing, and the Office informed all requesting parties about this fact. The Office also provided a number of telephone consultations and personal consultations regarding a record entered in SIS by another member state, with such request being, in compliance with EU regulations, forwarded to the supervisory authority of the responsible member state. One complaint regarding the processing of personal data in SIS was assigned to an inspector of the Office for investigation. The investigation was still not completed in 2013.

3 LEGISLATIVE ACTIVITIES

In 2013, a new key area of work in the field of legislation was the **Data Protection Impact Assessment ("DPIA")**, introduced into the legislative rules of the government in 2012. After many years of bustling legislative activity, which often did not take into account the specifics of work with information and privacy protection to a great degree, an instrument finally appeared in the Czech Republic, in the form of the DPIA, that reminds the people in charge of drafting regulations that they need to focus on implementing privacy protection rules already at the time of drafting plans and concepts, i.e., not by general proclamations about data protection with reference to Act No. 101/2000 Coll., but by describing and assessing the specific impacts of the proposed legislative solutions in existing and planned areas of personal data processing.

As part of the consultation procedure in respect of draft legislation, the Office attempted, in those cases where documents were presented to it, to identify key aspects of the intended personal data processing and propose the approach to take when drawing up DPIA, i.e., the obligation to explicitly state whether the proposed wording establishes a new personal data processing requirement, and if so, to justify the need for it and to describe its basic parameters: the purpose of processing, the category of processed personal data and key parts of the processing, namely the outputs of the processing and the personal data retention periods, with specifics and rules for publishing and accessing data on the Internet, which is so popular at this time.

With regard to the DPIA, it is not possible to accept draft legislation corresponding to information systems that were not set up in compliance with the principles for working with information and privacy protection (**Privacy by Design**).

The Office called attention to the need to draw up DPIA especially in the case of **registries (registers, records) with personal data**, which are kept by the public authorities. The legal regulation on maintaining registries is often very unspecific. Laws often contain only general mandates on maintaining registries, with the issue being delegated to implementing regulations, decrees or even the internal regulations of the registry administrator, which are usually not open to data subjects. Only to a limited degree is it possible to refer to the new Act on Public Registers of Legal Entities and Individuals, which

pertains to a number of specific databases. According to the case law of the Constitutional Court (e.g., Ruling No. Pl.ÚS 24/10 dated 22 March 2011 or Ruling No. Pl. ÚS 24/11 dated 20 December 2011) as well as of the European Court of Human Rights (e.g., Leander v. Sweden of 26 March 1987 or Amann v. Switzerland of 16 February 2000), the collection and retention of personal data is already an infringement of the basic right to privacy, with it not being decisive whether their further processing takes place or not. Personal data collection in registries kept by the state administration or local or regional government, as a rule with the consent of the individual concerned, is thus infringement of the right to privacy. The rules for such infringement should then be sufficiently regulated in the law. In 2013, in matters regarding registries, the Office, in the framework consultation procedure, provided guidelines for the drafting of legislation concerning a specific registry and required that the submitter of the bill always made it clear whether the proposed registry would be open to the public or not. The Office also often recommended that the registry be divided into a public and non-public part, along with specification of which information will be freely accessible. At the same time, it called attention to the obligation to clearly express the purpose for which the personal data should be made accessible and to the obligation to stipulate rules that ensure that the data are not presented in an inaccurate our outdated form. An example of a proposed improvement to a registry includes the requirements that the Office addressed to Ministry of Industry and Trade regarding the **Trade Licencing Register**. The Office proposed a more exact division of this register into a public and non-public part. The Office recommended placing restrictions on the publication of data that pertain more to the privacy of the entrepreneur than to his/her business activities – in cases where the businessperson states a business address that is different from his/her residential address, the residential address need not be made available in the public part of the register; furthermore, should the business address and residential address coincide, it is not necessary to state that the business address is in fact the same as the residential address.

In 2013, the Ministry of Health repeatedly called attention to the fact that the provisions of the Health Services Act were not duly substantiated and in the form approved do not provide an explicit guarantee that the processing of personal data will be in line with the law – the provisions are not even linked to the basic obligations set out in Act No. 101/2000 Coll. (in particular: the exactly defined purpose of processing, the proper legal reason for using the personal data, and the substantiated reasonable retention period). Without more specific rules, more doubts can be raised about the purpose and effectiveness of the entire NHIS and the transparency and credibility of the output from it.

In connection with its participation in public discussion on the draft **Cybernetic Security Act**, the Office was able to advance its comments calling attention to the fact that a necessary statutory condition for disposing of records according to this legislation will be the maintenance of electronic records in a way that will allow one to determine and verify when, by whom and for what reason data collected under this legislation was processed, including for how long and for what purpose they were retained (not excluding destruction protocols). The documentation on processing data used in the fight against cybercrime considers the personal data protection measures set out in Article 13 of Act No. 101/2000 Coll., which create the conditions for any required supervision and enforcement of the statutory obligation to maintain confidentiality, to be effective and technologically adequate.

As part of measures connected to the adoption of the Inspection Code, which the Office will begin to observe as of the beginning of the year, the **draft Personal Data Protection Act** was finalised and presented to Parliament for passage. With regard to the new assignment from the government to deal collectively only with issues that directly pertain to the Inspection Code, the most ambition part regarding the status of the board of inspectors was deleted from the new version of the bill. The procedure to be taken by inspectors as part of the board (e.g., discussion of objections against the inspection protocol) will thus be regulated, as was the case in the past, by the internal regulations of the Office.

With respect to one of the highest political priorities of the Czech Republic, i.e., **implementation of a public service system**, the persons responsible for drafting the respective legislation took into account the position of independent administrative bodies, of which the Office is one.

FOREIGN RELATIONS AND INTERNATIONAL CO-OPERATION

In 2013, just as in previous years, the Office devoted its energies to **discussions of the new European framework for privacy protection**, which have been going on almost continuously since January 2012. In addition to the directive on protection of individuals in connection with the processing of personal data by the respective authorities for the purpose of prevention, investigation, detection and prosecution of crimes or sentencing and on free movement of such data, discussions centred around the Regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (**General Data Protection Regulation**, the "GDPR")

In connection with the drafting of the GDPR, the Office called attention to the need to update and revise translation of GDPR terminology into Czech. With regard to the scope of the work, where finalisation of the GDPR in 2014 will be the task of the new EU authorities, the Office views negatively the fact that to date the general position of the Czech Republic to the GDPR has not been brought up to date.

The Office commented on the work around the GDPR through the advisory body of the European Commission, the **Data Protection Working Party (WP29)**, where the president of the Office is part of the management. Employees of the Office took part in five WP29 subgroups, which in 2013 drafted opinions not only on the above regulation and directive, but only on other issues, such as the current topic of cookies and "smart" devices and preparation and implementation of the innovative European directive on re-use of public sector information. The Office has traditionally taken part in special control group. An example is the Joint Supervisory Body of Europol.

Similarly, the representatives of the Office were active in joint supervisory bodies of some international information systems, namely the Schengen Information System, the Visa Information System, Customs Information System and the EURODAC system.

The Office's spokeswoman was involved in the Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) of the Council of Europe (T-PD) as its deputy chair.

Last year, in the area of international cooperation on projects, the Office continued with the **Leonardo da Vinci Partnership** programme. The objective is to provide employees (and employers) with practical information about their rights and obligations in connection with processing personal data in connection with employment (the official name of the event was "Raising awareness about data protection among employees working in the EU"). A team comprising experts from Bulgaria, the Czech Republic, Croatia and the Polish supervisory data protection authority is completing the text of a detailed handbook. In 2013, Office experts continued to give talks as part of foreign relations work – as part of a **study visit** from their colleagues from the Moldavian office under the title "Protection of personal data in printed and audio-visual media" and as part of expert support of the Moldavian Office for Personal Data Protection on the topic of cloud computing and data protection, at the European Data Forum 2013 conference in Dublin on the topic "Further use of public sector information and personal data protection", at the international data protection conference in Moscow on the topic "Personal data and mobile communications and applications" and **at the conference of the offices for personal data protection from Central and Eastern European countries** in Belgrade on a number of topics: independence of supervisory bodies, inspection in the field of automated personal data processing, and the obligations of employees in the area of electronic surveillance at the workplace.

In 2013, a new dynamic area of focus with a foreign element was cooperation on **responses to preliminary questions** (for the Czech Republic) being addressed **by the Court of Justice of the European Union**.

A proceeding on a preliminary question regarding Case No. C-212/13 Ryneš pertains directly to the Office. The subject of the assessment of the EU Court of Justice is whether the **operation of a camera surveillance system** located in a family house for the purpose protecting property, health and life of the home owners should fall under personal data processing carried out by a natural person in the course of a purely personal or household activity, in accordance with Article 3(2) of Directive 95/46/EC, even if such system is monitoring a public area.

OFFICE, MEDIA AND MEANS OF COMMUNICATION

The daily service provided to the media in 2013 satisfied the questions of journalists and provided responses within the shortest possible time, in most cases in one business day. The Office's website continued to inform about the Office's actual work, particularly on the homepage in the "News" column. A question from reporters which contained factual information on a transgression of Act No. 101/2000 Coll. or indicated a direct violation thereof become part of the Office's files as an instigation to initiate an investigation by the Office. Clearly even the media is very sensitive to personal data protection. Nevertheless, it is possible to register certain doubts on the part of the media concerning the Office's work. The media's approach to the application of the right to privacy and the right to access information often helps to devalue personal data protection.

A press conference organised on the occasion of the Personal Data Protection Day in January 2011 not only addressed this fundamental human right but also brought balance to the debate. Press conferences usually attract reports from the printed media - dailies and specialised publications – agency reporters, and representatives from the main radio and television stations. The outputs from press conferences have, as is usual, also appeared in a morning radio interview with the Office president and in the news at noon on the day of the conference. Whereas one to five reports concerning personal data protection in some way appear in the news every day, after the press conference in December 2013, 22 news reports were issued (not including short entries devoted to the press conference through interviews with the Office president).

An overview of the cases most closely monitored and the most serious issues is available on the Office's website in the "Press releases and conferences" and "Positions of the Office" columns.

RAISING AWARENESS ABOUT PERSONAL DATA PROTECTION

The Office, at the Personal Data Protection Day, which falls on January 28 each year, announced the 7th annual contest for children and youth "My Privacy! Don't Look, Don't Poke About!" ("Moje soukromí! Nekoukat, nešťourat!"). The information obtained from the contest, namely information concerning the youth's approach to using social networks, especially Facebook, showed that interest in protecting privacy on the Internet is minimal and that youth do not pay attention to even the minimum guarantees offered by social networks for personal data protection. At the same time, however, the work done by numerous experts, who special in the issue of youth and social networks, showed extensive knowledge and understanding of the issue; it appears, however, their work has not found a specific application, e.g., in lessons at school. However, it can be said with certainty that if digital literacy does not become part of the education process, which includes knowledge about personal data protection and privacy, their place in the context of fundamental human rights and individual freedom, no improvement in the young generation's approach to social networks can be expected.

To the extent possible, the Office supported the company Europe Generation and the publication of the Student Diary, which contains basic information about securing personal data protection on Facebook. Europe Generation distributed the Student Diary together with the Office's Information Bulletin, which was offered to educators together with the pamphlet on basic information about personal data protection.

The lecturing activities of the Office's employees were also extensive in 2013. Personal data protection as a special legal regulation was the subject of 33 lectures for state institutions, local government and entrepreneurs.

Round tables have become a new form of communication between experts and the Office Sector representatives who are obliged to fulfil the obligations imposed on them by Act No. 101/2000 Coll. thus have a direct opportunity to ask experts questions that ensue from their day-to-day practice, and the Office has the chance to explain its role as enforcer of Act No. 101/2000 Coll. In 2013, the round tables focused on "Modern trends in security technology from the point of the Personal Data Protection Act" and "Topical questions about personal data protection in relation to prevention and investigation of fraud within companies."

LIBRARY AND PUBLICATIONS OF THE OFFICE

The library provides support for employees of the Office. It is also open to professional public on request. It is used by students for their theses and dissertations concerning personal data protection. These papers are usually donated to the Office and become part of this highly specialised library.

In 2013, the Office published volumes 64 to 66 of its Journal. The Office has decided to begin publishing the Journal in electronic form only as of 2014.

In 2013, an issue of the Information Bulletin focused on the wide range of opinions of experts on the dangers that youth face on social networks was published.

WEBSITE OF THE OFFICE

The Office has decided to create a new website with more comprehensive search possibilities. Work began on it after the Office, through a discussion forum, examined the opinions and needs of the users of its website. The company Webhouse was chosen as the supplier. In addition to a more pleasant layout, the website has to allow experts and the general public to immediately obtain documents specifically focused on personal data protection. It also makes it possible to search for documents according to the various articles of Act No. 101/2000 Coll. and group them into a single overview. For the internal needs of the Office, the website introduces an effective editing and publication system. It will be launched in January 2014.

3

ORG INFORMATION SYSTEM

Act No. 111/2009 Coll., on basic registers, brought the Office the task of ensuring secure identification of citizens in the Basic Registers system via "source" and "agenda" identifiers of natural persons.

The result of this request was the creation and operation of the ORG Information System, which creates and submits "agenda" identifiers from one agenda to another and keeps a list of them.

The basic registers also contain other referential data on individuals (citizens), legal persons, self-employed individuals and public authorities, thereby simplifying and speeding up communication between people and the authorities.

At the end of 2013, the *basic registers have already connected* 2700 public administration information systems through which end users have access to data in the basic registers. The entire basic registers system operates 24 hours a day, 7 days a week. The scope of the basic registers system includes the registration of close to 400 agendas.

As of 1 July 2012, the ORG IS has been in operation and the number of processed transactions has been increasing. The marked increase in the number was due to this year's elections. In the election period, the number of transactions in the ORG IS increased three-fold compared to normal. The basic registers were used to create electoral registers for the various electoral districts. In September, the number of transactions was close to 20 million. The system was most burdened on 2 September 2013 when 2 720 950 transactions were processed. The average number of transactions per month is 13 262 758.

PERSONNEL OF THE OFFICE

The number of positions at the Office is determined by the state budget and has been set at 102 since 2010.

The employee fluctuation rate was around 10%, the same as last year. Employment contracts were concluded with ten new employees and terminated with nine. Of these, four retired and two went on maternity leave. The ten-year term of one inspector expired, so a new inspector was appointed in his place by the President of the Czech Republic.

As of 1 January 2013, the Office had 99 employees; as at 31 December 2013, this number was 100.

ECONOMIC MANAGEMENT OF THE OFFICE

The budget of the Office was approved by Act No. 504/2012 Coll., on the State budget of the Czech Republic for 2013.

Utilisation of state budget resources under Heading 343 - Office for Personal Data Protection

	in CZK thousands
Summary indicators	
Total income	11 881.33
Total expenditures	128 731.47
Specific indicators – income	
Total non-tax and capital income and accepted transfers	11 881.33
of which: total income from the budget of the European Union. excl. CAP	4 380.07
other non-tax and capital income and accepted transfers in total	7 501.26
Specific indicators – expenditures	
Expenditures to ensure performance of the tasks of the Office for Personal Data Protection	128 731,47
Cross-cutting expenditure indicators	
Salaries of employees and other payments for performed work	43 787.90
Mandatory insurance premiums paid by the employer*)	14 805.25
Contribution to the Cultural and Social Needs Fund	425.13
Salaries of employees within an employment relationship	34 246.50
Salaries of employees derived from salaries of constitutional officials	8 135.00
Total expenditures co-financed from the budget of the European, excl. CAP	1 871.00
of which: from the state budget	265.98
contribution from the EU budget	1 605.02
Total expenditures recorded in the information system of programme financing EDS/SMVS	17 644.03

*) social security and state employment policy premiums and health insurance premiums

Overview of state budget utilisation in 2013

Type of budget structure	Indicator	Approved budget 2013 in CZK thousands	Final budget 2013 in CZK thousands	Actual state according to financial statements as at 31 Dec. 2013 in CZK thousands	Actual/Final budget in %
4118	Non-investment transfers from the National Fund	571.00	571.00	4 282.29	749.96
4135	Transfers from the OUS reserve funds	0.00	0.00	72.21	
4153	Non-investment transfers received from EU	0.00	0.00	25.57	
2141, 2211, 2212, 2322, 2324, 3113, 4132	Other non-tax income	0.00	0.00	7 501.26	
	TOTAL INCOME	571.00	571.00	11 881.33	2 080.79
501	Salarie	42 409	42 421.50	42 381.50	99.91
5011	Employee salaries	34 244	34 256.50	34 246.50	99.97
5014	Employee salaries derived from salaries of government officials	8 1658	165.008	135.00	99.63
502	Other payments for executed work	2 055	2 056.40	1 406.40	68.39
5021	Other personnel costs	1 755	1 756.40	1 406.40	68.39
5024	Severance pay	300	300.00	0.00	0.00
503	Mandatory insurance premiums paid by employer	15 118	15 122.25	14 805.25	97.90
5031	Mandatory social				
	security premiums	11 116	11 119.12	10 864.12	97.71
5032	Mandatory public health insurance premiums	4 002	4 003.13	3 941.13	98.45

513	Purchase of materials	1 788	1 838.00	1 361.04	74.05
514	Interest and other financial expenses	15	15.00	11.07	73.77
515	Purchase of water, fuel and energy	2 430	2 645.00	2 160.19	81.67
516	Purchase of services	71 957	65 304.18	46 059.70	70.53
517	Other purchases	4 882	5 014.50	2 322.01	46.31
5171	Repairs and maintenance	1 714	1 714.00	524.07	30.58
5173	Travel expenses	2 300	2 372.21	1 404.05	59.19
518	Advances paid, principals	0	350.00	0.00	0.00
519	Expenditure related to non-investment purchases	2 269	2 621.93	2 316.66	88.36
5342	Transfers to Culture and Social Services Fund	424	427.13	425.13	99.53
536	Other non-investment transfers to other public budgets	17	54.50	48.78	81.51
542	Compensation paid to individuals	300	300.00	87.01	29.00
5424	Compensations paid during illness	300	300.00	87.01	29.00
	Total current expenditures	**143 664**	**138 170.39**	**113 384.74**	**82.06**
611	Intangible fixed assets under construction	4 200	5 114.30	5 114.06	100.00
612	Tangible fixed assets under construction	11 200	10 285.70	10 232.67	99.48
	Total capital expenditures	**15 400**	**15 400.00**	**15 346.73**	**99.65**
	TOTAL EXPENDITURES	**159 064**	**153 570.39**	**128 731.47**	**83.83**

Numerical data are taken from the financial statements compiled as at 31 Dec. 2013.

Overview of expenditures on projects co-financed from the EU budget in 2013

in CZK thousands

Name of project	Approved budget 2013	Final budget 2013	Actual state according to financial statements as at 31 Dec. 2013	Actual state/ /final budget in %
"Optimisation of OPDP Procedures"	672	1 830.55	1 773.22	96.86
Leonardo da Vinci "Raising awareness about personal data protection among employees working in the EU"		72.21	72.21	100.00
TAIEX		25.57	25.57	100.00
Total for projects financed by the EU	672	1 928.33	1 871.00	97.02

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

In 2013, the Office received a total of 79 requests for information. Compared to the previous year, this number represents an increase of almost 100%, as was then case of 2012 compared to 2011. The public's growing interest in the work of the Office is clearly a trend.

Of the total number of information requests, the Office fully satisfied 47, partially rejected 22 and fully rejected 10. Among the most frequent reasons for the partial or full rejection of information requests was protection of the personal data contained in the information requested, protection of information obtained during inspections (such information is protected by the law and subject to confidentiality), or the fact that the request concerned information that was not available to the Office.

In terms of content, most information requests pertained to the decisions of the Office. The requesting parties demanded either inspection conclusions or administrative decisions regarding certain categories of data controllers or more information in the case of proceedings that the Office, as the pertinent authority, initiated based on their prior instigation. A significant percentage of information requests pertained to the Office's spending, especially on hardware and software and on personnel and salaries.

COMPLAINTS HANDLING PURSUANT TO SECTION 175 OF THE RULES OF ADMINISTRATIVE PROCEDURE

The Office handled complaints pursuant to Article 175 in 2013 as well. Based on this provision, the affected parties are entitled to turn to the administrative body with complaints in the event they believe that the administrative body acted incorrectly or one its employees behaved inappropriately. The concept of complaints pursuant to Article 175 of the Code of Administrative Procedure serve to protect the rights of the affected parties if the law does not provide a different means of protection, which in particular means appeals and other ordinary and extraordinary legal corrective measures.

In 2013, the Office handled 41 complaints. These were assessed and then handled as complaints pursuant to Section 175 of the Code of Administrative Procedure. Of the complaints, 10 were assessed as warranted and 7 as partially warranted. The remaining 24 complaints were assessed as unwarranted. Compared with the previous year, the number of complaints continues to increase, albeit slightly.

The vast majority complaints related to disagreement with the handling of the prior instigation that the complainant sent to the Office and which concerned a suspected violation of Act No. 101/2000 Coll. In ten cases, a review of the complaint concluded that the Office did not proceed correctly when assessing the prior instigation from the complainant. In such cases, the complaint was forwarded either to the Office inspector who conducted the

inspection or the Administrative Proceedings Department to initiate administrative proceedings for suspicion of an administrative offence or transgression. In nine cases, the complainant turned to the Office with a complaint against the inspection conclusions of the Office inspectors or against how the inspection was conducted, with three complaints being deemed warranted in this case. One of the complaints concerned the procedure of the Registration Department in connection with registration proceedings; in this case, no violation of the law was ascertained. The respective department was informed in each case about the results of the complaint review process, and if it was discovered that its procedure was incorrect, even in part, it was asked to adopt measure that would prevent further complaints.

Of the 41 complaints in total, not a single one was against the inappropriate conduct of any official. This fact is, with regard to the number of instigations received each year by the Office, a very good finding and evidence that the Office when handling the received instigations, performing inspections and conducting administrative proceedings communicates with the public professionally and in compliance with the principle of good governance.

ANNUAL REPORT SUMMARY 2013
The Office for Personal Data Protection
Pplk. Sochora 27, 170 00 Praha 7
E-mail: posta@uoou.cz
Web: www.uoou.cz

In February 2014, 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.