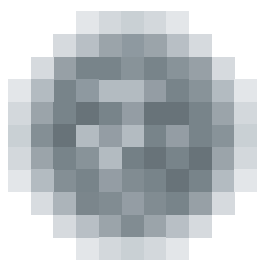


# Annual Report Summary 2014



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



# The President of the Office Looks Back



This is the tenth and last time that I will be presenting the annual report on the activities of this institution, which out of all public authorities has probably undergone the biggest changes both in terms of content and form. Just the legislation establishing our institution has been amended 25 times.

To begin with, there have been major advancements in the use of new technologies that have a strong impact on privacy. They allow for the collection, storage and extensive processing of personal data, not only instantly but also over the long term. At the time when I joined the Office, social networks, for example, did not exist.

New topics have arisen, such as efforts to ensure the secure transfer of personal data abroad to countries that do not guarantee sufficient protection of personal data, which is becoming a specific security issue with national and European implications. This point of view was clear to me having acted as Deputy Chairman of WP29, the expert body on personal data protection of the European Commission. I am certain that this issue, tied to cloud computing or profiling, for example, will be dealt with pressingly by the Office even after I step down as president in September 2015.

Further evidence that the work of the Office is beginning to change is the transformation of the level of quality of queries and especially consultation

requests that the Office receives from both individuals and corporate entities. The demanding nature of the work in this regard has clearly grown also thanks to the efforts being undertaken by the Office to raise awareness of personal data protection.

In this context, I have to say two things: on the one hand, some citizens try to misuse personal data protection to resolve their unrelated disputes – although the data protection law cannot and must not resolve such claims – mainly because of their greater legal awareness, but erroneous interpretation, of this legislation; on the other, law firms are trying to benefit from the Office's obligation to provide consultations free of charge. I would like to believe that the new tool being prepared in cooperation with the European Commission and the Council of Europe—“Handbook on European Data Protection Law”—which the Office website links to, can help to alleviate the demand of lawyers and the legal professional for time-consuming consultations. For the Office, such consultations require a large amount of time of a specific number of employees, and such time is not unlimited. The Czech version of the publication will appear next year. The publication will be intended primarily for lawyers who do not specialise in personal data protection, and will be easily accessible. It will provide a basis for understanding the rulings of the European Court of Human Rights and the Court of Justice of the European Union in Luxembourg in the area of protection of the European citizens' basic right to privacy.

In this connection, I have to mention the Office's many years spent trying to promote a balanced approach to protecting privacy and guaranteeing security. I worry, however, that often ill-considered solutions in the field of security will continue to be adopted in the fight against terrorism, which will cause privacy protection rights to deteriorate. This development has already been registered by the Office in connection with the modernisation of Convention 108, where the department of the Ministry of the Interior responsible for personal data protection began to apply pressure that security forces not just be subject to certain exemptions, but entirely excluded from any controls under the legal norms that a democratic Europe had taken a long time to implement. We are thus worried that efforts undertaken by the Office to have rules implemented for the police on how they should handle wiretap recordings, and thus to better protect privacy – an area for which the Czech Republic received a negative evaluation even from Privacy International – will come to naught. I am concerned that the many years of work by the Office and its inspectors to ensure that the police take a balanced approach to handling DNA profiles, an approach that would observe internationally adopted rules, may, in the context of the fight against terrorism, remain entirely without any regulation, and that calls by personal data protection advocates and genetics experts for the adoption of a rigorous law on DNA will again be postponed indefinitely (as has been the case since 2006 and again since 2011, with the situation now being urgent). I am just as worried about the use of camera surveillance systems, as the use of such systems is not regulated in the Czech Republic in any way.

In light of the good cooperation with the Ministry of Interior in connection with preparing the Czech Republic for its accession to the Schengen system, this experience does not fill me with joy, especially when I realise that if my fears come true, it will be proof of the deterioration of democracy and the unfortunate concessions we have made to the fundamentalist crusade against its values, with the protection of privacy and personal data being one of basic rights that had been enshrined while our democracy was being developed.

There are, however, a number of things that the Office managed to achieve that do fill me with joy. First and foremost, the Office has been able to fulfil the obligations arising from the new powers that have been gradually entrusted to it over the past nine years: managing its very

extensive agenda tied to prosecuting unsolicited commercial messages; and successfully fulfilling its supervisory duties related to the operation of the Schengen Information System, even by its employees involved in international cooperation, which was preceded by a positive international evaluation of the Office before the Czech Republic became a signatory to the Schengen Agreement. Another matter is securing a special part of basic registers, the backbone of the electronisation of state administration, which meant that Office had to build an entirely new security-demanding workplace. The Office also fulfilled its obligations during the Czech Republic's Presidency of the European Union without any problem. It also cooperated successfully with the Ministry of Industry and Trade at the Digital Challenges Conference in 2014, which is already an activity that is leading to a certain future. The road to improving personal data protection in the Cadastral Register and Trade Licence Register was also long, but successful nevertheless.

Strengthening the Office's position in international efforts began as early as 2005-2006, when the Office provided know-how under the European project for the long-term assistance to the Personal Data Protection Agency in Bosnia and Herzegovina. The Office also cooperated successfully with its Polish, Hungarian and Croatian counterparts: under the Leonardo da Vinci programme they worked together to develop two personal data protection handbooks in the area of employment. One of the publications is intended for entities doing business in the field of personal data protection and other addresses the issue from the point of view of employees and raises awareness on the rights and obligations tied to the protection of employee data.

The Office adopted and provided consultations to countless foreign experts. I should at least mention the visits made from Albanian, Romanian, Ukrainian and Chinese experts, the successful seminar for law students from the University of Chicago, and involvement in the telebridge between Czech and American high-school students organised by the American Cultural Center in Prague. The list could go on. In 2010, the Office organised the European Privacy and Data Protection Commissioners' conference, which was warmly received, also in part to venue: the Prague Castle. Also appreciated is the work of the Office's employees in international organisations – such as the supervisory body of Europol, the European Commission and its advisory body WP29, the Council of Europe and its advisory committee to Convention 108, and the Berlin Group – and their participation in the annual meeting of the group of supervisory authorities from Central European, Eastern European, Southern European and the Baltic countries to share findings from supervisory activities. This meeting is an appropriate platform to share experience with personal data protection in states that have had experience with totalitarian regimes and the consequences of such a history on creating an environment respecting the protection of privacy. The Czech and Polish offices were the founding members of this group.


I should not forget to mention the international award that the Office received in Madrid in 2007 for the best project in the field of education in personal data protection, which also received accreditation from the Ministry of Education, Youth and Sport for three years running. Each year, the Office also organises a contest for youth and children called "My Privacy! Don't Look, Don't Snoop!" ("Moje soukromí! Nekoukat, neštourat!"), which was part of the honoured project and which is receiving ever growing support in schools and even in the media and is gaining ever more partners. Similarly, the Office organises round tables with experts who have to deal with personal data protection requirements in their businesses or work (security agencies, law firms, the media) and fulfils perfectly its role in promoting dialogue helping to enshrine personal data protection as a necessary component of a well-functioning society that respects the freedom and rights of each individual.

Last but not least, I have to praise the work of the Office's employees. I have found them to be an exceptionally cooperative, professional, moral and able-bodied team. I greatly appreciate that the inspectors who joined the Office in 2011 were able to organically build on the work of their predecessors, and that as new issues arose, the supervisory activities and cooperation among the inspectors developed as well.

The participation of external experts in the work of the Appeals Committee, which is my advisory body, was beneficial even in terms of the balance of legal opinions used by the Office to promote one of the basic human rights in the Czech Republic. My wish is that access to personal data protection be balanced and that this balance be strengthened, and I state this with the knowledge that personal data protection has of late been curtailed especially due to the emphasis on the right of access to information.

I also wish that Office will be able to integrate the Civil Service Act next year without much ado to help fulfil the purpose of the Personal Data Protection Act, which is service to the citizens of a democratic state.

Dear Senate, I would like to thank you for the excellent cooperation and for helping the Office retain its independence, which is exemplary within the European Union.



Igor Němec

# CONTENTS

THE OFFICE IN NUMBERS 2014	10
SUPERVISORY ACTIVITIES OF THE OFFICE	13
<b>SUPERVISORY PLAN</b>	14
1. Information systems with large amounts of data	14
2. Impact of new technologies on personal data processing conditions	15
3. Observance of the conditions of the Schengen legal framework	16
4. Other areas of investigation under the supervisory plan	16
5. Review of the fulfilment of imposed remedial measures	18
INSPECTIONS INITIATED UPON INSTIGATION OF THE PRESIDENT OF THE OFFICE	19
FINDINGS OBTAINED BY INSPECTORS IN SUPERVISORY ACTIVITIES	23
<b>I. SUPERVISORY PLAN</b>	23
Processing of personal data of applicants and recipients of grants from the State Environmental Fund	23
Processing of personal data of patients in electronic form via hospital information system	24
Employee monitoring	25
<b>II. INSPECTIONS INITIATED UPON INSTIGATION OF THE PRESIDENT OF THE OFFICE</b>	30
Protection of personal data processed within the Customs Information System (CIS) and in the Customs Files Identification Database (FIDE)	30
Inspection of the use of dynamic biometric signatures	33
Investigation into the application of the Central Electronic Payment Order	34
Processing of personal data in the insolvency register	35
Inspection of the processing of personal data of motor vehicle owners and operators in the AUTOTRACER system (VIN processing)	36
<b>III. INSPECTIONS ACCORDING TO VARIOUS THEMATIC GROUPS</b>	40
A. Personal data processing via monitoring systems at places of work, in means of transport and in residential buildings	40
Camera surveillance systems in residential buildings	40
Camera surveillance systems in public transit	41
B. Processing of sensitive data in connection with the provision of health care services	43
Loss of a patient's medical file in Lužice Hospital	43
Content of data in a medical evaluation	45

Processing of personal data of the clients of a health insurance company during their pre-registration	45
C. Personal data processing in registries of debtors	46
Personal data processing on www.dluzis.cz and in the SOLUS debtor registries	46
D. Energy service providers and the processing of clients' personal data	50
Observance of the obligation of personal data processors with focus on the data subjects' consent when concluding agreements through general business terms and conditions	50
E. Separate contributions	51
Inspection of www.scio.cz, s.r.o.	51
Lists of association members	53

## OTHER SUPERVISORY ACTIVITIES 57

## COMPLAINTS HANDLING AND CONSULTATIONS 57

## SOME FINDINGS OBTAINED IN ADMINISTRATIVE PROCEEDINGS 61

Proceedings under Article 17 of Act No. 101/2000 Coll.	61
Option not to impose a fine	62

## FINDINGS FROM JUDICIAL REVIEWS 64

Video monitoring in the workplace is only possible in cases where the purpose cannot be fulfilled using less intrusive means; periods for processing of the recordings also have to be adapted to this purpose. Fulfilment of the notification obligation under Article 11 of Act No. 101/2000 Coll. is dependent on the group of persons being monitored. In case of doubt, the personal data controller should request a consultation pursuant to Article 29(1) of Act No. 101/2000 Coll.	64
---	----

Traffic and location data recorded and stored pursuant to Article 97(3) of Act No. 127/2005 Coll., on electronic communications, may not be made accessible by reference to Article 40(1)(a) of Act No. 121/2000 Coll., the copyright act	66
---	----

If the inspected entity aims to call attention to the fact that they were imposed obligations that do not correspond to the actual state of affairs, it is necessary for them to do so immediately via objections to the inspection protocol	66
--	----

Preparation of television reports aimed at publishing of personal data through television broadcasting constitutes personal data processing pursuant to Act No. 101/2000 Coll.	67
--	----

Expending all efforts that may be required in accordance with Article 46 of Act No. 101/2000 Coll. does not mean any efforts expended by the data controller, but, in relation to each specifically evaluated case, maximum possible efforts that the controller is able to expend objectively. Thus, the fact that a concluded works	
---	--



contract contained a detailed description of the procedure, from the takeover of specific waste from a controller by another responsible person, is not a sufficient reason for relieving one of liability	67
<b>REGISTRATION</b>	69
<b>TRANSFERS OF PERSONAL DATA ABROAD</b>	72
<b>SCHENGEN COOPERATION</b>	76
<b>LEGISLATIVE ACTIVITIES</b>	79
<b>FOREIGN AFFAIRS AND INTERNATIONAL COOPERATION</b>	83
<b>OFFICE, MEDIA AND COMMUNICATION TOOLS</b>	87
Raising awareness about personal data protection	87
Office library and publications	88
Office website	89
<b>ORG INFORMATION SYSTEM</b>	90
<b>OFFICE PERSONNEL</b>	91
<b>ECONOMIC MANAGEMENT OF THE OFFICE</b>	92
<b>PROVISION OF INFORMATION PURSUANT TO ACT NO. 106/1999 COLL., ON FREE ACCESS TO INFORMATION</b>	94
<b>COMPLAINTS HANDLING UNDER SECTION 175 OF THE CODE OF ADMINISTRATIVE PROCEDURE</b>	96

# THE OFFICE IN NUMBERS 2014

<b>Inquiries and consultations</b>	Inquiries in the Czech Republic	2965
	abroad	35
	out of which	
	for state administration	148
	for local governments	191
	for legal persons	498
	for natural persons operating a business	344
	for natural persons	1819
<b>Pleadings and complaints</b>	instigations received pursuant to Act No. 101/2000 Coll.	1536
	complaints referred to inspection or administrative procedure	237
<b>Unsolicited commercial communications</b> (competence pursuant to Act No. 480/2004 Coll.)	total instigations	7951
	instigations resolved	5792
	inspections initiated	23
	inspections completed	14
	administrative decisions on a fine	8
	challenged by objections	12
	objections accepted	0
	objections dismissed	10
	mostly accepted	0
mostly dismissed	2	
<b>Inspections</b> (excluding inspections concerning Act No. 480/2004 Coll.)	initiated	144
	completed	128
	referred to other governmental authorities	3
	challenged by objections	11
	objections accepted	1
	objections dismissed	7
	mostly accepted	0
	mostly dismissed	4
	analyses	34

<b>Administrative punishment</b>	administrative proceedings for violation of Act No. 101/2000 Coll. and Act No.133/2000 Coll., on Population Register	78
	infraction proceedings pursuant to Act No.101/2000 Coll.	17
	administrative and infraction proceedings pursuant to Act No.13 101/2000 Coll. – Article 44 a, 45 a	10
	infraction proceedings for violation of Act No. 159/2006 Coll., on conflict of interests	0
	appeal decision on legal violations	32
	appeals dismissed	20
	cancelled and returned to new hearing	2
	cancelled decisions and discontinued proceedings	5
	change in the decision	6
<b>Judicial review</b> <i>NB: * in total since 2001)</i>	court actions lodged	10 (128*)
	actions dismissed by the court	4
	decisions cancelled by the court	9
	court proceedings closed/pending since 2001	88/40
<b>Registration</b>	notifications received (pursuant to Article 16 of Act No. 101/2000 Coll.)	7686
	instances of processing registered	7392
	still pending	1001
	registrations cancelled	132
	notifications on a change in the processing	845
	proceedings pursuant to Article 17	134
	discontinued (no violation)	106
	discontinued for procedural reasons (e.g., notifications withdrawn)	13
not permitted	4	
<b>Authorisations for transfers of personal data abroad</b>	accepted applications for transfers of personal data abroad (pursuant to Article 27 of Act No. 101/2000 Coll.)	40
	decisions on authorisations of transfers	30
	decisions on dismissal	0
	proceedings discontinued for procedural reasons	8
<b>Notifications pursuant to Act No.127/2005 Coll.</b>	notifications received	2

Complaints pursuant to Article 175 of the Code of Administrative Procedure	complaints received	39
	complaints found justified	10
	complaints found partly justified	5
	complaints found unjustified	24
Applications pursuant to Act No. 106/1999 Coll.	applications received	74
	fully accepted	43
	partially accepted	23
	applications rejected	8
Materials published	Office Journal (number of volumes)	2
	Information Bulletin (number of volumes)	1
Legislative drafts on which comments were made	laws	81
	implementing regulations	53
	draft government regulations	15
	draft decrees	38
	other	61
	foreign materials	13

# SUPERVISORY ACTIVITIES OF THE OFFICE

The Office for Personal Data Protection (the “Office”), which was established in line with the legal framework of the European Union as an independent supervisory authority to check the observance of personal data processing obligations of accountable bodies, focused in 2014 on certain significant trends and activities of the accountable bodies in connection with the use of modern technologies to process the personal data of employees, clients, patients, grant recipients and other categories of natural persons (individuals).

The intentions of the accountable bodies, which are often legally established for the primary purpose of data processing, are often combined and take on the form of collecting and then using personal data for a purpose that substantially differs from the primary purpose, even though the accountable body does not possess a licence for such secondary processing.

Through its supervisory plan, which is developed to cover a specific period of time, the Office also uses findings from its investigations conducted in previous periods which showed that the collection of personal information and its subsequent evaluation with the aim of profiling individuals from various angles of their lives and then distributing this information for marketing purposes was and continues to be a long-term trend of many business entities. Such conduct, however, is also prevalent in the public sector, where citizens can turn to the state with a request for certain services, assistance in the form of social contributions, lease of a council flat, provision of certain tax relief or waivers of fines etc., and in this connection have to provide information and documents on living conditions.

The existence of databases currently termed “big data” cannot be traditionally linked only to public bodies or entities such as big banks and insurance companies. Data ownership means being responsible for protecting such data. For this reason, the Office focused more thoroughly on the way personal data was safeguarded against unauthorised access and handling.

When implementing the supervisory plan, inspectors and their teams focused on the following general topics:

# • SUPERVISORY PLAN

## I. INFORMATION SYSTEMS WITH LARGE AMOUNTS OF DATA

Extensive information systems with large amounts of data have long been the subject of supervision by the Office. Each year, the Office chooses different areas and in this way can compare how the rights and obligations of the accountable entities are observed. By doing so, it can compare the level of application of Act No. 101/2000 Coll., on Personal Data Protection, in the various sectors. In 2014, inspection of the following databases took place:

### 1.1. Central electronic payment orders:

The Office aimed to check the register of electronic payment orders and other record-keeping tools and files that are maintained by the electronic order management system as well as all other activities related to the system that take place exclusively through computer technology. For this purpose, courts use appropriate software (the Central Electronic Payment Order application – “CEPR”), which is managed by the Ministry of Justice.

The outcome of the inspection was as follows:

One important finding was that periodically imposed and into practice implemented measures eliminate to a sufficient degree the risk of unauthorised access to processed personal data and prevent systematic errors.

In light of the above, it was concluded that neither an inspection of the Ministry of Justice, as the operator of the CEPR application, nor an inspection of a randomly selected user of this application, namely the Klatovy Regional Court, ascertained any violation of Act No. 101/2000 Coll.

More information on the course and results of the inspection can be found in the section Findings Obtained by Inspectors in Supervisory Activities.

### 1.2. Implementation of operational and grant programmes:

1.2.1. The Office chose the Klidné přihraničí (Peaceful Borderlands) project, which Sdružení obcí mikroregionu Šumava (the Šumava Micro-region Association of Municipalities) intends to implement, for its supervisory activities in 2014. The inspection should have focused on the observance of the obligations of data controllers in connection with the installation and operation of preventive measures and elements contributing to the safety and fluency of road traffic and its monitoring.

As the preparation of the project, including the approval procedure, was delayed, it was decided to defer the commencement of the inspection until the next monitoring period.

1.1.2. Based on the supervisory plan of the Office for 2014, an inspection of the Ministry of Education was started. The subject of the inspection was the observance of the obligations of a data controller under Chapter II of Act No. 101/2000 Coll. in connection with personal data processing in documentation related to the grants of the Ministry of Education, Youth and Sports announced as State Support for Sports for 2013 and 2014.

The inspection is still underway.

### 1.3. Processing of the personal data of bank clients:

Banking and financial services are a traditional area for the Office's supervisory plans. Even though assessment of the observance of obligations is not always received with due respect, the Office has always tried to promote such rules that do not discriminate clients.

In 2014, the inspection focused on Sberbank CZ, a. s.

The outcome of the inspection was as follows:

The inspection focused on the observance of the obligations of the data controller when communicating with clients in situations where the personal data of the clients is collected and processed in connection with the services offered by the bank and conclusion of contracts. The purpose of this process is the fulfilment of contractual terms and conditions.

The inspection, which commenced in 2004, demonstrated a breach of the inspected entity's obligations under Article 11(1) of Act No. 101/2000 Coll. In connection with the inspection findings, the Office plans to start negotiations with the Ministry of Interior on eliminating the current problems with interpreting the ban on making copies of personal identification cards that contain machine readable data.

### 1.4. Operation of state funds in connection with personal data protection:

In 2014, the Office focused on the State Environmental Fund of the Czech Republic established by Act No. 388/1991 Coll., on the State Environment Fund of the Czech Republic, as the body managing funds that can be used, inter alia, to support the investment and non-investment efforts of legal and natural persons related to protecting and improving the environment.

The outcome of the inspection was as follows:

The database of aid recipients/applicants maintained by the SEF in electronic form was safeguarded in line with Act No. 101/2000 Coll.; the disclosure of the personal data of aid applicants and recipients to third parties does not take place without legislative backing; as regards the transfer of data abroad as part of aid from the European Union, such transfer did not take place prior to or during the inspection.

More information on the course and results of the inspection can be found in the section Findings Obtained by Inspectors in Supervisory Activities.

Another fund where the processing of personal data was examined in 2014 in connection with the operation of an information system with a large amount of data was the State Cultural Fund of the Czech Republic, established by Act No. 239/1992 Coll., on the State Cultural Fund, which provided funding in the form of special-purpose aid, loans or non-repayable financial aid for organising cultural festivals, shows and similar cultural events, for supporting cultural projects aimed at preserving and developing the culture of national minorities in the Czech Republic or for supporting highly worthwhile non-professional artistic activities. The inspection is still underway.

## 2. IMPACT OF NEW TECHNOLOGIES ON PERSONAL DATA PROCESSING CONDITIONS

During 2014, an agreement was reached within the WP29 technological subgroup on the joint testing of cookie-based technology. Cookies are small data files stored on a user's device when

visiting a website. In this way, users leave a trace of their activity in the Internet environment. Cookie operators can then obtain useful information about the user.

In connection with a WP29 document and an agreement on technological procedures, the current practice of a number of providers of electronic communication services was reviewed, with focus on published terms and conditions and personal data protection policy.

A test was conducted in 2014 based on which the Office drew up a basic analysis which will be starting point for further supervisory activities. The analysis showed, inter alia, that the fulfilment of the obligations in relation to the use of cookies is generally not adequate among Czech website operators. It is also clear that the current situation in the Czech Republic does not correspond to either European or Czech (insufficiently transposed) legal regulations, and Internet user rights are thus being systematically violated.

The Office, as the regulator, will be addressing this situation in the next period as well through its supervisory activities.

### 3. OBSERVANCE OF THE CONDITIONS OF THE SCHENGEN LEGAL FRAMEWORK

#### 3.1. Review of the operation of the Visa Information System:

Like every year, the Office reviewed the observance of the conditions of the Schengen Agreement for granting Czech visas to foreigners. As part of this review, where the inspected body was the Ministry of Foreign Affairs, two on-site inspections were carried out: an inspection of the consular office attached to the Embassy of the Czech Republic in Georgia located in Tbilisi and an inspection of the consular office attached to the Embassy of the Czech Republic in Egypt located in Cairo.

The outcome of the inspections was as follows:

The review of the Tbilisi consular office was aimed at the fulfilment of the obligations of a data controller, especially with regard to the fulfilment of Article 11 of Act No. 101/2000 Coll. when notifying data subjects, and the data controller's obligations in connection with safeguarding personal data pursuant to Article 13 of Act No. 101/2000 Coll.

In this connection, the inspector stated that both the data controller's notification duty and the way the data controller safeguarded the personal data carriers were fully in line with Act No. 101/2000 Coll.

More information on the course and the results of the inspection of the embassy in Cairo can be found in the Schengen Cooperation section.

### 4. OTHER AREAS OF REVIEW UNDER THE SUPERVISORY PLAN

#### 4.1. New-born screening – an inspection is being conducted on the basis of an instigation by the Iuridicum Remedium association:

The inspection focused on assessing valid legal regulations on the conditions for collecting and processing sensitive data on the state of health of new-borns. The Office thus also focused in its



supervisory activities concerning the legal conditions for processing sensitive data on new-borns and submitted its proposals during the consultation procedure regarding the new draft of the decree of the Ministry of Health on medical documentation.

Due to its scope, the inspection has still not been completed.

#### 4.2. Employee monitoring at workplace:

Further to certain findings and available information regarding the possible monitoring of the behaviour of employees at their place of work by the employer with the aim of preventing damaging behaviour at the workplace, an on-site inspection took place at ŠKODA AUTO a.s. and at Plzeňský Prazdroj, a. s.

The outcome of the inspections was as follows:

The inspected entities stated that the camera surveillance systems with recording equipment are operated in line with Section 5(2)(e) of Act No. 101/2000 Coll., as they are necessary for the protection of the controller's rights and the controller's interests protected by the law. Both companies duly fulfilled their duty to notify their employees and third parties as required by Article 16 of Act No. 101/2000 Coll. The inspection did not ascertain any breach of any other obligations imposed on camera surveillance system operators by the above-referenced legislation.

More information on the course and results of the inspection can be found in the section Findings Obtained by Inspectors in Supervisory Activities.

#### 4.3. Observance of the obligation of data controllers with focus on the details of the consent of data subjects when concluding general business terms and conditions:

The inspection was aimed at companies with activities regulated by a special law. Three entities were checked: RWE Energie, s.r.o., ČEZ Prodej, s.r.o., and O2 Czech Republic a.s.

The inspection of RWE Energie, s.r.o. commenced in 2013 and ended in 2014.

More information on the course and results of the inspection can be found in the section Findings Obtained by Inspectors in Supervisory Activities.

#### 4.4. Reviews of certain data processing procedures that were the subject of proceedings under Article 17 of Act No. 101/2000 Coll.:

##### 4.4.1. Dopravní podnik města Brna, a.s., with regard to the specific use of collected data

More information on the course and results of the inspection can be found in the section Findings Obtained by Inspectors in Supervisory Activities.

#### 4.5. Processing of the personal data of a data controller's clients in connection with the operation of a sports centre.

The outcome of the inspection was as follows:

The inspection of World Class Czech Republic s.r.o. focused on how this sports centre was maintaining its client database in connection with the services being offered in the field of sports and the related accompanying services. The inspectors assessed the findings and stated that there was a breach of Articles 11 and 16 of Act No. 101/2000 Coll.

## 5. REVIEW OF THE FULFILMENT OF IMPOSED REMEDIAL MEASURES

As part of monitoring adherence to the conditions by accountable bodies, an inspection of the Prison Service was conducted in 2014 with the aim of monitoring how the accountable body fulfilled the measures imposed on it based on the results of a previous inspection, which had focused on processing the personal data of prisoners in connection with maintaining the central register and identifying prisoners.

The outcome of the inspection was as follows:

The inspection did not reveal any breach of the obligations of the inspected entity pursuant to Act No. 101/2000 Coll. in connection with maintaining the register and identifying prisoners. The inspectors did however recommend that the inspected entity adopt an internal regulation that would unify the methodology used to identify prisoners in all of the inspected entity's organisational units. The inspected entity accepted the recommendations.

More information on the course and results of the inspection can be found in the section Findings Obtained by Inspectors in Supervisory Activities.

# • INSPECTIONS INITIATED BASED ON AN INSTIGATION OF THE PRESIDENT OF THE OFFICE

## 1) National Registers Authority (“NRA”)

The inspection was aimed in particular at the fulfilment of the NRA’s duties in connection with personal data processing in line with Act No. 101/2000 Coll. and at the fulfilment of the NRA’s obligations under Article 7(5) of Act No. 111/2009 Coll., on basic registers, according to which the NRA should inform the Office for Personal Data Protection if it has warranted doubts that a public authority is handling personal data without authorisation.

The inspection should also have assessed the NRA’s procedures under Article 58 of Act No. 111/2009 Coll. which regulates the NRA’s duty to notify natural persons/data subjects when disclosing data about them from the Register of Inhabitants and the Register of Rights and Responsibilities of Public Authorities. The inspection is still underway.

## 2) 5P Agency

The inspection focused primarily on the observance of the data controller’s (processor’s) obligations under Article 5(5) et seq. of Act No. 101/2000 Coll. when collecting and subsequently processing not only the contact information of customers who are natural persons. At the same time, it was expected that the outcome of the inspection would assess the impact of the processing of the contact data of the company’s employees and self-employed persons in connection with questions repeatedly posed by the Office in relation to the privacy of employees/natural persons and self-employed persons and expressed in the Office’s opinions, especially in Opinion No. 3/2011 “Protection of Personal Data of Natural Persons Operating a Business”.

Inspection results:

The inspection found that the inspected entity processes the personal data of natural persons, even self-employed persons, listed in the database of the data controller (the client) for the purpose of offering business and services. The inspection did not find that the inspected entity, as the data controller, processed the personal data of natural persons. As the inspected entity was a data processor, the provisions of Article 6 of Act No. 101/2000 Coll. have to be observed, i.e., the data controller has to conclude a personal data processing agreement with the data processor if the authorisation to process personal data does not ensue for the processor from a legal regulation.

The inspection found that the inspected entity processed personal data based on a personal data processing agreement concluded with the data controller pursuant to Article 6 of Act No. 101/2000 Coll. In the agreement, due attention was paid to setting out guarantees by the processor concerning technical and organisational safeguards in place to protect personal data.

The inspected entity, as the personal data processor under Article 4(k) of Act No. 101/2000 Coll., did not process the personal data of natural persons for the client at variance with the processor’s obligations under Act No. 101/2000 Coll.

### 3) Ministry of Foreign Affairs

The inspection focused on fulfilling personal data protection conditions when processing personal data as part of visa proceedings at embassies, especially in connection with notifying data subjects about their rights under personal data protection regulations, and on the procedures in place for verifying and safeguarding personal data processing under the visa information system (VIS).

None of the previous reviews of processing of personal data in connection with visa proceedings at embassies had been aimed directly at the transfer of the personal data of short-term visa applicants to the VIS.

For this reason, this time the inspection also focused on the transfer of personal data to VIS, as this also ensues from the recommendations of the Schengen Evaluation Working Group (SchEval) in the personal data protection section, from the meetings of the Coordination Group for Supervision over VIS and from the need to provide due protection of personal data in connection with its processing in VIS on the national level as well.

More information on the course and outcome of the inspection can be found in the Schengen Cooperation section.

### 4) Ministry of Transport, prospectively the Czech Insurers' Bureau (Česká kancelář pojistitelů)

The aim of the inspection was to verify in what way the inspected entity obtains and subsequently processes data in the Central Motor Vehicle Register (the "CMVR"), the operator of which is the inspected entity in line with Article 5 of Act No. 56/2001 Coll., on the conditions for the operation of vehicle on roads. It also focused on whether and in what way the inspected entity observes its obligation to process only exact personal data obtained in compliance with this law when processing the personal data that it receives and, if necessary, to update such data in compliance with Article 5(1)(c) of Act No. 101/2000 Coll. in conjunction with Article 8 of the same.

Inspection results:

The inspection found that the incorrect data that the Central Motor Vehicle Register had contained in the past and that the Czech Insurers' Bureau had been referring to when collecting and enforcing insurance was being corrected on a continuous basis and was being amended and supplemented by the public authorities using a new connection to the Basic Register Information System and by personal contact with the persons concerned and even with ATS-TELECOM Praha a.s., the company "cleaning" and sorting the processed data. At the same time, the entrusted authorities (registration points) conducted administrative proceedings to remove discrepancies in the data kept in the CMVR. Until resolved, each case was conducted separately and marked with a comment in the CMVR. The results of the proceedings were then reported to the Czech Insurers' Bureau in accordance with Article 15(11) of Act No. 168/1999 Coll., on liability insurance for damage caused by operation of a vehicle.

The inspected entity amended and supplemented the personal data in the CMVR via the registration points and even the public registers. The inspection did not ascertain any breaches of Act No. 101/2000 Coll. At the same time, the relevant legislative amendments were implemented by the Ministry of Transport during the inspection. The most important amendment concerns a change in the conditions for making changes to a vehicle owner's registration when deregistering and registering a vehicle at the same time.

**5) With regard to the Prague Municipal Court and other identified regional courts that make decisions in compliance with Article 7a of Act No. 192/2006 Coll., the Insolvency Act,** as the court of first instance in insolvency proceedings, the inspection focused primarily on observing the obligations of the data controller (processor) when collecting and subsequently processing the data of debtors and their creditors while implementing the proposal for commencing and conducting insolvency proceedings in line with the Insolvency Act.

When examining the conditions for collecting and processing personal data, including its disclosure, it was necessary to focus on the application of Article 422 of Act No. 192/2006 Coll., which states that upon the request of the natural person who lodged the petition, the insolvency court may decide that some of the applicant's personal data contained in the petition will not be made public in the insolvency register. If the person in question is not the natural person that lodged the petition, only the name and surname of such natural person is to appear in the insolvency register. In such case, the insolvency court is to append to the filed petition information about the nature of the personal data that is not to be made public.

Inspection results:

The inspection found that other persons are not always redacted (made anonymous) in the public documents of the insolvency register in compliance with Article 422(2) of Act No. 192/2006 Coll. The conclusion of the inspection protocol thus states that Act No. 101/2000 Coll. was breached.

From the assessment of the facts, the inspection did not find that the inspected entities processed (collected) personal data of natural persons in insolvency proceedings above and beyond the scope stipulated in Act No. 192/2006 Coll.

With regard to the legal assessment of the facts ascertained by the inspections conducted, the issue of publication (disclosure) of personal data and the redaction thereof in the insolvency register will be discussed with the Ministry of Justice, as there are ambiguities in interpretation of the process and problems with implementing it in practice.

**6) General Customs Directorate – in connection with the operation of the customs files identification database (FIDE) and the Customs Information System (CIS)**

More information on the course and results of the inspection can be found in the section Findings Obtained by Inspectors in Supervisory Activities.

**7) Cebia, spol. s r.o.**

More information on the course and results of the inspection can be found in the section Findings Obtained by Inspectors in Supervisory Activities.

**8) Air Bank a.s.**

More information on the course and results of the inspection can be found in the section Findings Obtained by Inspectors in Supervisory Activities.

**9) A – GIGA s.r.o.**

The inspection focused particularly on the observance of the controller's obligations when collecting and subsequently processing the personal data of customers under the conditions set out in the agreement concluded by and between the inspected entity and the Prison Service of

the Czech Republic regulating the conditions for operating a civilian call centre for supporting the sales of A-GIGA established and operated in the Vlnařice prison.

Inspection results:

The inspection has been completed. No breach of Act No. 101/2000 Coll. has been ascertained.

#### **10) Google Czech Republic, s.r.o.**

The inspection examined compliance of the inspected entity's procedures with the conditions of Act No. 101/2000 Coll. and with the declared intention as per the notification made to the Office as part of registration proceedings in April 2011.

The inspection was conducted in connection with the ruling of the Court of Justice of the European Union in the case of Google v. Costeja of 13 May 2014. It is clear that in compliance with Article 4(1)(a) of Directive 95/46/EC of the European Parliament and of the Council that the domestic branch (establishment) in the Czech Republic should be the entity responsible for the above processing and such establishment should focus all of its activities on all natural persons living in such state. In the Office's opinion, in line with the mentioned ruling, the basic mission of this establishment is the support of the sale of Google Inc. products or the sale of advertising space offered as part of related services (e.g., search engine services).

The aim of the inspection was to examine the procedures used by the inspected entity when accepting requests of the affected natural persons to remove their names from search engines and the method of verifying the identity of applicants.

Inspection results:

The inspection is still underway.

#### **11) Statutory City of Plzeň**

In connection with an instigation by the ombudsman that pertained to the issue of the rules of allocating flats owned by the City of Plzeň in relation to an equal and fair approach to housing, the inspection focused on the New Rules for Disposing of Flats and Non-Residential Premises and the Conditions for Selecting Tenants for Vacant Flats in Buildings Owned by the City of Plzeň.

Although these rules cannot be considered outright discriminatory according to the ombudsman, the requirements of Act No. 101/2000 Coll. do have to be taken into account however.

A separate issue that the inspection should have checked was whether the demands on the scope of the obligatorily disclosed, and in this connection processed, personal data pertaining to flat applicants/future tenants are in compliance with the cited legislation.

Inspection results:

The inspection is over and it was found that Act No. 101/2000 Coll. has been breached, specifically its Article 5(1)(d): in order for the flat applicants to be included on the waiting list, applicants had to submit their extract from the Criminal Register, which the inspected entity then retained. This approach has been changed.

As the inspected entity remedied the detrimental situation still during the inspection, the inspector decided to proceed in compliance with Article 40a of the cited legislation. The Ombudsman's Office was informed of the results of the inspection.

# • FINDINGS OBTAINED BY INSPECTORS IN SUPERVISORY ACTIVITIES

## I. SUPERVISORY PLAN

### Processing of the personal data of applicants and recipients of funding from the State Environmental Fund

As part of the Office's supervisory plan for 2014, the State Environmental Fund of the Czech Republic (the "SEF") was inspected. The subject of the inspection was observance of the obligations of the controller/processor of personal data under Chapter II of Act No. 101/2000 Coll. in connection with the fulfilment of the obligations ensuing from the appropriate personal data protection regulations, especially when processing the personal data of entities applying for and receiving funds from the SEF.

Pursuant to Article 1a of Act No. 388/1991 Coll., on the State Environment Fund of the Czech Republic, the SEF can process the personal data of aid applicants only in the scope required to carry out the task in question.

In this way, controls are in place at the SEF for checking the accuracy of the data provided in aid applications. If any incorrect or missing data concerning aid applicants is discovered, the aid applicant is, as a rule, asked to supplement the inaccurate or missing data, or the inaccurate/missing data is corrected/supplemented directly in the inspected entity's register. The provision of aid as part of the various subsidy programmes is governed by the appropriate directives of the Ministry of the Environment (the "MoE"). Aid applicants or aid beneficiaries, which include natural persons, are obliged to submit documents – stipulated by the respective MoE directive or binding instructions for fulfilling the aid conditions – with their aid applications in connection with the application administration procedure and implementation of the project.

Aid applications (other than in the case of National Programmes) with the filled in personal data and required copies of documents containing personal data are submitted electronically via an on-line form available on the website of the respective programme, e.g., in the case of the Nová zelená úsporám (New Green Savings) programme on <http://www.nova-zelenausporam.cz>.

In the case of National Programmes, applications are submitted in writing to the SEF mail room together with the obligatory annexes and these are then also converted into electronic form. The MoE is obliged in accordance with Article 1(11) of Act No. 388/1991 Coll. to publish the minister's decision on the use of the resources of the inspected entity. The list of natural and legal persons, i.e., aid beneficiaries, that the minister decided to award a specified amount of aid to, is thus also published on the SEF website along with the following personal data: name, surname, municipality, region where the project is to be implemented, aid amount, and MoE decision number. Within the National Programme, the application acceptance number, under which the agreement to grant aid is then recorded, is then indicated in the list of aid beneficiaries in the case of group decisions. Pursuant to Act No. 218/2000 Coll., on budgetary rules [Article 3(a) and Article 18a], the SEF, as the aid provider, transfers the personal data of

applicants and beneficiaries to the central aid register maintained by the Ministry of Finance. The Ministry of Finance is obliged to publish documents and data regarding the provision of grants and non-repayable financial aid on its website for at least 10 years regardless of facts that occurred even after such publication [Article 18a(6) of this same].

Data about beneficiaries are further passed on to the following bodies: General Financial Directorate into the central register of subsidies – CEDR – on a quarterly basis pursuant to Article 75b of Act No. 218/2000 Coll., in the scope stipulated by a decree of the Ministry of Finance; the Ministry of Finance (only in the case of applications financed or co-financed through the State budget); Evidenční dotační systém (EDS), the programme financing information system, which implements the conditions of Decree No. 560/2006 Coll. of 11 December 2006, as amended by Decree No. 11/2010 of 7 January 2010 effective as of 19 January 2010; the *de minimis* aid register (only if the attributes of public aid are met) pursuant to Act No. 215/2004 Coll., on regulation of certain relationships within the area of State aid and on amendments to the Act on the Support of Research and Development and implementing Decree No. 465/2009 Coll., on data recorded in the central register of *de minimis* aid, allowing not only information about subsidies and beneficiaries to be entered but also data about the total amount of aid provided in the Czech Republic to be viewed and the total amount of aid granted to a specific subject to be ascertained, so that it is possible to verify the amount of funding provided for the respective period. Data about beneficiaries is also available to applicants under Act No. 106/1999 Coll., on free access to information.

Each programme has its own special database from which only the lists of aid beneficiaries that received a decision from the Minister of the Environment, i.e., accepted and approved subsidy requests, are disclosed, with the SEF updating these lists on its website on an ongoing basis.

The SEF is not authorised to disclose the list of aid applicants and beneficiaries, including the personal data of data subjects, to anyone else but the public authorities and criminal authorities under a special law. In criminal proceedings, the SEF has already provided the requested documents concerning a specific applicant or aid beneficiary to the criminal authorities.

With regard to the inspection, it can be stated that the database of aid applicants/beneficiaries maintained by the SEF in electronic form was duly safeguarded in compliance with Act No. 101/2000 Coll., that the personal data of aid applicants and beneficiaries is not provided to third parties unless required under the law, and that, as regards transferring data abroad as part of inquiries from the European Union, no such transfer took place prior to or during the inspection.

### Processing of personal data of patients in electronic form via hospital information system

As part of the Office's supervisory plan for 2013, two randomly chosen hospitals were inspected: Nemocnice Rudolfa a Stefanie Benešov, a.s., and Nemocnice Tábor, a.s. (the "Hospitals"). The inspections of these Hospitals were completed in 2014. During the inspection, the observance of the data controllers' obligations under Act No. 101/2000 Coll., with a focus on the processing of the personal data of patients contained in the medical records maintained in electronic form via the hospital information system and on safeguarding the medical records.

The way the Hospitals handled the medical records and the system used by them to secure their respective information systems were checked physically. The inspectors focused on observance of the provisions of Article 13 of Act No. 101/2000 Coll., i.e., on stipulating and



fulfilling the technical and organisational measures of the Hospitals, as the controllers of the patients' personal data maintained in the medical records, especially with regard to the right granted to medical personnel to access the medical records maintained in electronic form; on checking the right to access to the medical records; and on archiving the medical records.

It was found that Nemocnice Rudolfa a Stefanie Benešov, a.s. tracks access to its automated systems (even remotely) as well as any changes made in the automated systems. Such access is randomly checked, with such control taking place if it is discovered that access to the medical records of one patient is frequent. The Hospital also ensures that its automated system is accessed only by authorised persons. The inspection did not ascertain any breach of Article 13(4) of Act No. 101/2000 Coll. The inspection protocol concluded that the Hospital when processing personal and sensitive data in medical records maintained in electronic form via the Hospital's information system and when safeguarding such information, did not breach Act No. 101/2000 Coll.

The inspectors' findings with respect to Nemocnice Tábor, a.s. were similar. The Hospital also did not breach Act No. 101/2000 Coll. when processing personal data contained in medical records kept in electronic form via the Hospital's information system and when safeguarding such data.

The above inspections concluded that the level of safeguarding of the medical records kept in electronic form was high and that authorisation granted to medical personnel to access the medical records was divided up according to their specialisations, and checks regarding authorised access were performed regularly. At both Hospitals, numerous external experts contributed to the operation of the information system, with the obligations under Act No. 101/2000 Coll. being observed. In the inspectors' experience, this confirms the fact that in connection with the lack of a national electronic health care system, the Hospitals, and all health care facilities providing services in compliance with Act No. 372/2011 Coll., on health care services, are forced, as part of efforts to develop their electronic system, to ask numerous external suppliers not only to provide the respective system, but also to operate and maintain it.

### Employee monitoring

Based on an analysis of supervision practices, the issue of monitoring employees at the workplace and in the employer's common areas was one of the primary areas addressed by the Office's supervisory plan for 2014. The Office based the supervisory plan on the qualified assumption that there is substantial latency in the wrongful conduct by employers also due to the fact that a substantial share of complaints from employees were anonymous. The situation on the job market, which is affecting the whole of society, played a role here.

At the same time, it needs to be stated that in numerous cases the content of a complaint was not found to be credible. Especially in the case of unsuccessfully job applicants or released employees, revenge could have been the motivation for them in a number of cases to file complaints with the aim of causing problems for the company, as data controller, including the possibility of its having to pay a fine.

In the period from 9 September to 3 November 2014, based on the Office's supervisory plan for 2014, an inspection of ŠKODA AUTO a.s. was conducted. The subject of the inspection was observance of the obligations of personal data controllers under Chapter II of Act No 101/2000 Coll. when processing personal data in connection with monitoring employee

at their workplace and in the employer's common areas. Practically the same inspection, also with respect to the subject matter thereof, was conducted in the period from 10 October to 30 November 2014 at Plzeňský Prazdroj, a. s.

The findings from the inspections at both companies were divided up methodologically into various areas, in which it was possible to assume that the employer's activities could be designated as the monitoring of employees at their workplace and in the employer's common areas.

#### S e l e c t i o n   p r o c e d u r e

The inspections did not prove any breach of internal procedures, which observe the respective provisions of the Labour Code. The forms and documents used in the selection (hiring) procedure only contained personal data required for the subsequent conclusion of an employment contract, i.e., name, surname, date of birth, place of residence, attained level of education and position sought at the company. Once the selection procedure ended, the personal data of the unsuccessful candidates was destroyed. The inspections concluded that the inspected entities did not breach in any way the provisions of Article 5(1)(d) and (e) of Act No. 101/2000 Coll., i.e., the obligation to collect personal data in the scope corresponding only to the stipulated purpose and to store such data only for the period required to process it.

#### S t a f f   m a n a g e m e n t

Both inspected entities had drawn up work rules that also contained a separate chapter on the protection of the personal data of employees. The employees' personal files were stored in the appropriate way (lockable office and filing cabinets) in the human resources department. Only persons authorised under the Labour Code, i.e., essentially senior managers and HR managers, had access to them. The manner of handling personal files and documents is based on the respective generally binding legal regulations (the Archives Act) and internal regulations (Filing Rules). In this connection it was stated that both entities paid due attention to fulfilling their obligations under Article 13 of Act No. 101/2000 Coll., i.e., adopting and documenting such measures that would prevent unauthorised access and misuse of the personal data of employees.

#### E m p l o y e e   I D   c a r d s

At both companies, every employee received a multi-purpose card. Such card contained the employee's photograph, name and surname and chip codes. The cards were the property of the company, but the holders were responsible for their proper storage and protection, and their loss had to be reported immediately. The cards allow access to the company's premises, access to specific workplaces and protected zones; are used to purchase foods and record working hours; have the function of an electronic signature; and are used for coding and signing into electronic mail according to the indicated level of authorisation (reading, writing, deleting etc.). Only authorised persons, i.e., senior managers and HR and Payroll Department staff, had access to data on working hours. The records were stored in compliance with the employer's obligations under general binding legal regulations to keep an overview of employee working hours. Cardholder obligations and other details are addressed in the respective internal regulations of ŠKODA AUTO a.s. and Plzeňský Prazdroj, a. s.

### A t t e n d a n c e   s y s t e m s

The arrival of employees to all of the plants of both of the inspected companies, i.e., in Mladá Boleslav, Kvasiny, Vrchlabí, Plzeň, Nošovice and Velké Popovice, and even to specific workplaces, was recorded via the multi-purpose cards. Each senior manager could check to see if their employees had entered the main gate, which is important at the moment when production lines are to start up and an employee is not at their place. According to granted authorisations, card-holders should have access to various protected zones. Each entry and exit is logged. The system in use was fully functional. No other measures to check working hours or the presence or absence of an employee in a specific space -- something that is very important in case of evacuation in the event of an emergency, fire or other incident -- need to be adopted.

Every visitor to the main plant of ŠKODA AUTO a.s. in Mladá Boleslav receives the document "Important Information for Entering Škoda Auto Grounds" at the entrance gate for pedestrians. The visitors' identity cards are scanned (only necessary personal data, i.e., not the photograph, signature, personal ID number or information about relatives). They receive a visitor's card that allows them to move about on the grounds in connection with the workplace of the person they are visiting, who also has to accompany them. The card is not transferable and is returned when leaving the grounds. Loss of or damage to a card has to be reported to the Security and Trademark Protection Department. Plzeňský Prazdroj, a. s. receives hundreds of visitors -- domestic and foreign -- every day. These visitors are taken on tours by tour guides. Movement outside the public part of the plant, i.e., in the various workplaces, is only possible based on coded access dependent on the specific employee authorisations encoded in the chip of the multi-purpose cards.

### C a m e r a   s u r v e i l l a n c e   s y s t e m s

All plants of ŠKODA AUTO a.s. were equipped with independent camera surveillance systems with recording equipment, electronic security and fire alarms and perimeter protection. The on-site inspection at the Mladá Boleslav and Kvasiny plants examined whether all monitored premises were duly designated as such by information signs with a camera symbol and accompanying text in both Czech and English. The monitoring system is not used to check employee work performance. It is only used to protect property and to prevent and detect criminal activity. The only place with central access to the entire camera system is the crisis management room, which is only accessible to the system administrator. Significant authorisation is given to internal security staff and staff of the "Central Security Desk". Recording are only passed on to the Security and Trademark Protection Department staff and to the criminal authorities.

The on-site inspection at the plant of Plzeňský Prazdroj, a.s. in Plzeň found that cameras monitor the parking lot in front of the building, entrances into the plant grounds, courtyard, entrances to specific buildings, outdoor warehouses, loading and unloading areas and the outside perimeter of the entire grounds. Inside the building, the cameras monitor the automatic cash desk, bottling lines and automated production areas. Information signs with the camera symbol and contact data for the administrator are located at all entrance gates and in front of the entranceways to the buildings in which cameras are installed. The views of the outdoor cameras are transmitted on-line to the monitors of the "monitoring centre" at the central security desk. Only one device was able to make a copy of a recording. The monitoring centre is

managed by an external security agency, which provides security services for the Prazdroj building. Only a limited number of people had access to the recording equipment and each access was logged.

For both inspected camera system operators, it is a matter of course that premises where personal activities take place (locker rooms, showers, toilets) are excluded from monitoring. A general principle is that employees are not recorded at times when they are not obliged to work (e.g., during breaks) and in premises designated for rest. Both ŠKODA AUTO a.s. and Plzeňský Prazdroj, a. s. are fully aware of the respective conditions under Section 316 of the Labour Code that allow for the continuous monitoring of employees at the workplace. To date, there has been no major complaint made by an employee concerning unauthorised or unlawful monitoring at the workplace. Each intent to monitor a workplace is first discussed with the trade union. All camera systems with recording equipment are registered by the Office.

With regard to the above, the inspectors stated that the camera systems with recording equipment are operated in line with Article 5(2)(e) of Act No. 101/2000 Coll., as it is necessary for the protection of the data controllers' rights and legally protected interests. Both companies duly fulfilled their duty to notify their employees and third parties as required by Article 16 of Act No. 101/2000 Coll. The inspection did not ascertain any breach of any other obligations imposed on camera surveillance system operators by the above-referenced legislation.

#### Internal periodicals and other publications

The employees of both inspected entities provided their consent to the publication of their personal data, including photographs, in internal publications.

#### GPS in company vehicles

Only two vehicles of the internal security services at the main plant in Mladá Boleslav and one vehicle at each of the plants in Vrchlabí and Kvasiny were equipped with GPS equipment. The vehicles were labelled accordingly and do not leave the company grounds. The aim of this measure is for the staff operating the "Central Security Desk" to have a continuous overview of where the vehicles are located and in case of an incident are able to contact the nearest vehicle as required. The team driving the vehicle have of course been informed about the use of the GPS equipment. GPS equipment is not used in standard manager and referential vehicles.

The company vehicles of Plzeňský Prazdroj, a. s. were equipped with GPS equipment with an "on and off" function, with the "off" function being used to differentiate between business and private trips. The GPS unit primarily served to records trips via an electronic trip log book. It also provided active protection of property (monitoring operation of the vehicle and increasing safeguards against theft) and allowed for the creation of electronic payment orders and subsequent accounting of travel costs, including fuel. The inspector concluded that the inspected company does not infringe on employee privacy, or need not take place through a simple action that is dependent on the free will of data subjects: switching the private/business trip button.

#### Internet and electronic mail

The content of the organisational standard "IT Security" builds on Volkswagen's IT Security Policy. The security rules serve to protect the credibility, integrity and availability of information

as well as to preserve the rights and interests of the company and all natural and legal persons that are in a business or employment relationship with the company. Electronic mail was regularly examined for the presence of unsolicited messages. Creating, sending and forwarding unsolicited chain or bulk business or private messages is forbidden.

Employees who need access to the internet for their work have it and can only use it for work-related purposes. Certain areas, e.g., access to paid sites, are blocked. The company has control mechanisms in place that are able to reveal various degrees of unusual and excessive behaviour. It is possible to ascertain the time, duration and even specific website visited or to reveal private e-mails with high-risk key words. Such control of course does not fall under mail secrecy. In the past, there have been a number of cases where access to the internet had to be dealt with. This sensitive area is described in detail in the methodological guidelines of ŠKODA AUTO a.s. entitled "Control of Data Stored in Information Systems". The methodological guideline entitled "Recording data on Information System Operation" then states that: "All information systems and the components used in ŠKODA AUTO a.s. have to allow data about activity, i.e., "logging", to be recorded. Minimum data in the log include the operation initiation indicator, date and time of the operation and its specifications. The logs are stored in a central repository for at least three months as of the record date. In the case of systems with a higher logging level, i.e., with classified company information, the logs are stored for 12 months.

The employees of Plzeňský Prazdroj, a.s. who use a PC for their work can also use the internet to a reasonable degree even for private purposes. The company blocks internet pages with inappropriate content across the board. Internet use by employees is not monitored; there is however restricted access for the individual workstations depending on the work they do. Managers have remote access to the network of Plzeňský Prazdroj, a.s. The details are address by the internal IT guideline for use.

The conclusion of the inspection in this area was that both companies pay strict attention to the observance of mail secrecy, as a constitutional right, and are aware that violation of this right can be prosecuted under criminal law.

#### Data Loss Prevention systems

Data Loss Prevention (DLP) systems are not made use by the companies at this time with regard to the scope and meaning of this term. ŠKODA AUTO a.s. is considering making use of it in the future. At this time, a similar system is being developed where the current system logs or, more precisely, prevents unauthorised copying of protected know-how on external media.

In conclusion, both inspections scheduled in the Office's supervisory plan for 2014 fulfilled their purpose. They contributed in a significant way to obtaining relevant information important to the Office for deciding on the direction of its supervisory activities in the next period. The Office is pleased to state that the "major" employers possess the means and the staff to adequately protect the person data of their employees. They are aware of the risks of unlawful monitoring of employees at the workplace or in the employer's common areas and are interested in observing valid legal regulations, including the provisions of Act No. 101/2000 Coll.

## II. INSPECTIONS INITIATED BASED UPON INSTIGATION OF THE PRESIDENT OF THE OFFICE

### Protection of personal data processed within the Customs Information System (CIS) and in the Customs Files Identification Database (FIDE)

Based on the instigation of the President of the Office, an inspection was conducted of the Customs Information System ("CIS") and Customs File Identification Database ("FIDE"), both of which are managed in the Czech Republic by the Customs Administration of the Czech Republic or, more precisely, the General Customs Directorate ("GCD").

The subject of the inspection was observance of the data controller's/processor's obligations under Chapter II of Act No. 101/2000 Coll. in connection with the fulfilment of obligations ensuing from the respective personal data protection regulations by the Customs Administration of the Czech Republic, as the group of administrative bodies and armed security forces or, as the case may be, the General Customs Directorate, as the controller of the personal data processed under the Customs Information System (CIS) and the Customs File Identification Database (FIDE). The inspection was aimed particularly at the technical and physical personal data safeguards in place, including the rules and procedures for processing, storing and destroying personal data, ensuring the protection of the rights of data subjects contained in the CIS and FIDE, securing information about access to personal data (logs) and measures to prevent the unauthorised processing of personal data.

As part of international cooperation among the customs administrations of the Member States of the European Union, which together provide supervision over the various customs territories of the European Union based on a common customs legislation, the common Customs Information System and Customs File Identification Database are used.

The purpose of CIS is to help prevent, investigate and detect operations that are at variance with customs or agricultural regulations of the European Union or are serious violations of the national regulations of the Member States of the European Union, by improving the efficiency of cooperation and supervision by the appropriate authorities of the EU Member States through the rapid dissemination of information. CIS comprises two central databases: CIS EU and CIS MS (MS = Member State). These are managed by the European Anti-Fraud Office (OLAF). The difference between CIS EU and CIS MS depends on whether the information is entered into them based on the legislation of the European Union or the legislation of the various EU Member States.

The CIS also contains a special database called Customs File Identification Database (FIDE), which is also divided up into FIDE EU and FIDE MS. The objective of FIDE is to help prevent operations that are at variance with customs regulations and agricultural regulations related to goods that enter or leave the customs area of the EU, and to facilitate and accelerate their detection and prosecution. The purpose of FIDE is to allow the European Commission and the appropriate authorities of the Member States responsible for customs inspections, provided they are initiating an investigation or are investigating one or more persons or enterprises, to ascertain which authorities of the other Member States are investigating or have investigated

the person or enterprise in question, so that based on information on the existence of a investigation file they can better achieve their objectives. The CID/FIDE databases include the following personal data, i.e., it is possible to enter the following personal data into them: surname, surname at birth, first name, former surnames and pseudonyms; date and place of birth; nationality; sex; number, place and date of issue of identification documents (passport, identity card, driver's licence); address; special objective (visible) and permanent physical features; reason for entering information; proposed measure; warning code calling attention to previous experience with weapons, violence or escape; and vehicle registration number.

Pursuant to Article 4(5) of Council Decision 2009/917/JHA of 30 November 2009 in conjunction with Council Framework Decision 2008/977/JHA of 27 November 2008, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life are not entered under any circumstances. Processing is permitted only when this is strictly necessary and when the national law provides adequate safeguards. The inspection found that such personal data is not processed by the General Customs Directorate as national laws do not regulate such processing as required by international regulations.

The CIS/FIDE systems are accessed through the AFIS Portal interface, which is managed by OLAF. In the framework of the AFIS Portal, CIS is implemented in the MAB (Mutual Assistance Broker) application, which also allows for the safe and secure exchange of requests for mutual assistance among Member States of the European Union. FIDE, on the other hand, is subordinated to the AIF Portal only. The GCD possesses no technical or operational documentation to CIS/FIDE, as it is only a client/user of CIS/FIDE; being the end user, it only has the possibility to store shared data and cannot intervene in communication routes between the OLAF Centre and user accounts and vice-versa.

Registered CIS users who have been granted a user ID and password have direct access to records in CSI or to the MAB/CIS terminals. GCD service regulations specify those departments of the Customs Administration of the Czech Republic that can enter records into CIS EU and CIS MS, including the authority to enter queries into CIS through registered users. Access to CIS/FID for the purpose of entering new records/queries is only possible from service computers, and only by approved users who have been allocated a user name and password. Double authorisation is required in order to access data. Each user is categorised into groups which classify members according to roles in the CIS/FIDE systems. Only a limited number of users possess special privileged access.

In addition to officers of the Customs Administration of the Czech Republic, other authorities that are authorised accordingly under national legislation have access to data in CIS or the right to enter requests for execution of certain measures. For CIS EU, such authorities are the Ministry of Agriculture, Ministry of the Environment, State Agricultural and Intervention Fund, phytosanitary and veterinary supervision authorities, Police of the Czech Republic, public prosecution authorities and the courts. For CIS MS, such authorities are the Financial Analytical Unit of the Ministry of Finance, the Police of the Czech Republic, public prosecution authorities and the courts. Specifically, access to data in CSI is used only by the customs officers of the Customs Administration of the Czech Republic.

PCs of standard configuration used in the Customs Administration of the Czech Republic serve as MAB/CIS terminals. MAB/CIS terminals must not be connected to the web interface.



Printing documents from CIS is possible only on printers located in the same room or near to the MAB/CIS terminals.

OLAF is responsible for the management of MAB/CIS on the central level. It is responsibly particularly for client software and the central database. The Directorate-General for Taxes and Customs Union is responsible for the CNN/CSI communication network. The GCD is responsible for the communication network in the framework of the Customs Administration of the Czech Republic and for establishing accounts on the CNN/CSI national gateway for internal purposes. The GCD is responsible for the local configuration of MAB/CSI workstations on the level of the GCD and on the level of the various customs offices with regard to the specific data stored in workstations.

The accuracy/correctness of data entered into CIS/FIDE is guaranteed because data is entered based on the prior discovery of a violation of customs regulations, where such violation is documented in the respective recording-keeping systems of the Customs Administration of the Czech Republic (e.g. Warning Duty). The data in the prior record-keeping systems is accurate because a protocol was drawn up with the person who violated the pertinent regulations and their personal data had thus already been verified. In the case of CIS, this fact is confirmed upon entering the case into CIS. When beginning to enter the record in CIS, it is necessary to state "source type" and "evaluation of information". With regard to this fact, it is stated by the records entered into CIS that the "information originated from an official source", "the source has been assessed as reliable" and "the assessed information was correct".

Records entered into CIS have to contain information about the validity period and are stored only for the amount of time necessary for achieving the purpose for which they were entered into CIS.

For the purposes of FIDE, in the case of files pertaining to ongoing investigations, records must not be stored for more than three years if no violation of legal regulations is discovered, six years if a violation of regulations was discovered but no prison sentence or fine was imposed, and ten years if the investigations led to a prison sentence or fines being imposed. Data from FIDE are deleted automatically once the respective maximum retention periods expire.

The inspection findings showed that personal data is entered in compliance with the stipulated purpose especially for the purpose of allowing any customs authority within the European Union to examine whether there is warranted suspicion that a specific person, vehicle or product violated EU customs or agricultural regulations or warranted suspicion of the gross violation of national legislation. Personal data is entered into CIS/FIDE only in the scope necessary to fulfil the stipulated purpose and is processed only in compliance with security measures on secure computers in the possession of the Customs Administration of the Czech Republic. The Customs Administration of the Czech Republic or the GCD fulfil its respective personal data protection obligations under Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agriculture, as amended, Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, Act No. 17/2012 Coll., and Act No. 101/2000 Coll. CIS users observe all personal data protection measures, including security measures, that are set out in the service regulations of the Customs Administration of the Czech Republic.



## Inspection of the use of dynamic biometric signatures

Based on an instigation of the President of the Office, an inspection was performed of Air Bank a.s.

The subject of the inspection was the observance of the obligations of personal data controllers/processors under Chapter II of Act No. 101/2000 Coll. by Air Bank a.s. ("Air Bank" or the "inspected entity") in connection with the processing of personal data of Air Bank clients who, when signing agreements or addenda, provide their signature using the SignPad device or a similar device that processes dynamic biometric signatures.

Pursuant to Article 5(1)(a) and (b) of Act No. 101/2000 Coll., the data controller is obliged to stipulate the purpose, means and method of processing of the personal data in question. The obligation arising under this provision is one of the basic principles predetermining the extent of other obligations connected to the subsequent processing of personal data.

The inspected entity's internal document entitled "Personal Data Processing Information" states that the above data is used to clearly identify users of Air Bank services. Signatures provided via the SignPad device are also listed as personal identification data in the document.

Handwriting and a signature are considered to be unique to each individual. A detailed analysis of a signature can be used to process various information about the movement of the hand when the signature was provided, such as the angle, pressure, speed, size of handwriting etc. This information can then be used by experts to identify or authenticate the person in question. This information or dynamic traits correspond to the definition of biometric and, thus, sensitive data in accordance with Act No. 101/2000 Coll. A classical signature captured on paper as well as dynamic biometric signatures contain the corresponding sum of information (angle, pressure, speed etc. of the handwriting), and are thus the carriers of biometric data.

When assessing the further application of Act No. 101/2000 Coll., one has to proceed with respect to what is mentioned above about data processing. Obtaining and retaining a signature without using it as a piece of sensitive data therefore cannot be considered processing of sensitive data if the biometric characteristics are not further utilised. Such processing only occurs if the signature is, for example, subject to detailed graphological analysis for the purpose of verifying its authenticity in case of a dispute.

In its written response to the findings of the inspection, the inspected entity enters the signature directly into the PDF form of the contractual documents at the moment the signature is recorded using the SignPad. The client and the bank see the signature only in graphic form. In order for the biometrics of the signature to be analysed further, it is necessary to own deciphering software and know the respective hash (key). According to the inspected entity's written response, the inspected entity does not own or use deciphering software at this time.

A condition for each attempt at processing is the existence of legal grounds to undertake such processing. Pursuant to Article 5(2) of Act No. 101/2000 Coll., personal data processing can take place either upon the data subject's consent or based on one of the other legal grounds laid down in letters (a) to (g) of such provision. If the dynamic biometric signature is processed to the same extent, in the same way and for the same purpose as a classical signature, it is possible to apply in particular the legal grounds stipulated under Article 5(2)(b) of Act No. 101/2000 Coll., which pertains to processing to the extent required to conclude an agreement where the data subject is a party thereof or to negotiate the conclusion of or amendment to an agreement upon the data subject's proposal.

The inspection did not ascertain any breaches of the provision of Article 5(1)(a) and (b) or Article 5(2) of Act No. 101/2000 Coll. The fine line treaded on in the use of this technology needs to be stressed, as any other steps leading to the use and processing of sensitive data, such as the automatic use of biometric data for verifying the signature of a client would already be subject to the stricter regime under Article 9 of Act No. 101/2000 Coll.

### Investigation into application of the Central Electronic Payment Order

Based on the inspection findings from incident controls and with regard to the substantial amount of personal data processed when issuing electronic payment orders by the courts, inspection of personal data processing in the Central Electronic Payment Order (Centrální elektronický platební rozkaz - "CEPR") was scheduled in the Office's supervisory plan for 2014. The CEPR application provider, and thus the data controller, is the Ministry of Justice.

The inspection of this entity was carried out in the period from 13 February to 25 June 2014. As the data controllers are all CEPR users, i.e., the district and regional courts, the inspection included examination of the procedure used to issue electronic payment orders at the randomly chosen Klatovy District Court. The subject of the inspection was the observance of the obligations imposed on data controllers and processors under Article 101/2000 Coll.

In the case of natural persons, a proposal to issue an electronic payment order contains personal data in the following scope: name, surname, date of birth, personal identification number, place of residence and, in the case of petitioners, also the amount of the claimed financial amount and banking data, including bank account numbers.

The inspection found that the CEPR application was introduced based on the Agreement on the Maintenance and Support of Information Systems of the Ministry of Justice concluded between the Czech Republic - Ministry of Justice and CCA Group a.s. on 16 March 2011. Article 9 of the agreement - "Safeguarding Information" – states that the supplier undertakes to safeguard confidential information under such agreement and to observe the obligations under Act No. 101/2000 Coll. The procedures for issuing electronic payment orders are detailed in the user handbook "Central Electronic Payment Order" dated 26 February 2014. It was checked whether the technical solution adopted by CCA Group a.s., which has long been working with the Ministry of Justice, is not in fact creating the conditions for any unauthorised processing of personal data.

As regards meeting the obligations under Article 13 of Act No. 101/2000 Coll., the inspection found that the Ministry of Justice has long had in place and documented technical and organisational measures to ensure the protection of personal data, to prevent access by unauthorised persons to means that would allow the processing of such data, and to determine and verify to whom the personal data was disclosed. The users of the CEPR application (the courts) have in place internal regulations concerning the procedure and liability of designated persons authorised to process personal data set out in the proposal to issue an electronic payment order, including access to the Central Inhabitants Register.

Each access to the CEPR application is logged. It is required that the respective form be labelled with the file number of the respective case file into which it is then filed. It is thus easy to ascertain who accessed the Central Inhabitants Register via the CEPR system, when and why.

One important inspection finding was that ordering and implementing periodical control

measures in practice to a sufficient degree eliminates the risk of unauthorised access to processing personal data and prevents errors of a systematic nature.

With regard to the above, it was concluded that the inspection found no evidence that the Ministry of Justice, as the operator of the CEPR application, or the randomly chosen user of such application, i.e., the Klatovy District Court, breached Act No. 101/2000 Coll. in any way.

### Processing of personal data in the insolvency register

Based on the complaint received and on the instigation of the President of the Office, two inspections were conducted at a Municipal Court (“MC”) and at a Regional Court (“RC”)

in compliance with Section 7a of Act No. 182/2006 Coll., on insolvency and its resolution (the Insolvency Act), as the courts of the first instance in insolvency proceedings. The inspections were aimed at the observance of the obligations of the data controller when collecting and further processing the personal data of debtors and their creditors when implementing insolvency proposals and conducting insolvency proceedings in compliance with Act No. 182/2006 Coll., especially with regard to the application of Section 422 of Act No. 182/2006, under which the insolvency court may decide, at the request of the natural person who lodged the proposal, that some of the personal data pertaining to this natural person contained in the lodgement will not be available to the public in the insolvency register. The inspection of the MC and RC discovered a breach of Act No. 101/2000 Coll., namely of Article 5(2) and (3). When processing personal data (collecting, redacting, disclosing), the courts proceed under special legal regulations on insolvency proceedings and under Act No. 101/2000 Coll. Information about data subjects collected in the insolvency proceedings are personal data in accordance with Article 4(a) of Act No. 101/2000 Coll. Personal data processing without the data subject’s consent is necessary for fulfilling the legal obligations controlled under Act No. 182/2006 Coll., and Article 5(2)(a) of Act No. 101/2000 Coll. Insolvency proceedings, including the insolvency register, personal data processing and the redaction of such data are regulated by Act No. 182/2006 Coll., Decree No. 311/2007 Coll., on the rules of procedure for insolvency proceedings, which implements certain provisions of Act No. 182/2006 Coll., and Instruction of the Ministry of Justice Ref. No. 505/2001-Org. – internal and office rules for district, regional and high courts.

The inspection found that the application and interpretation of Section 422(1) of Act No. 182/2006 Coll. (redaction of personal data in connection with a request filed by a natural person and a request for redaction and subsequent disclosure) are problematic in practice and that the courts did not always redact all documents in insolvency proceedings. Due to the ambiguous interpretation of this provision of Act No. 182/2006 Coll., personal data pertaining to such natural persons are published in other parts of the insolvency register.

The first sentence of Section 422(1) of Act No. 182/2006 Coll. (...at the request of the individual who has made the appropriate filing, the insolvency court may decide that some of the personal data of such natural person contained in the filing will not be available to the public in the insolvency register. Such a request may be made at any time during the insolvency proceedings. The insolvency court will always publish the name and surname of such natural person in the insolvency register.) allows for a dual interpretation regarding redaction. It can be deduced from this provision that only the personal data indicated in the natural person’s request should be redacted, not the same personal data that may be contained in other documents

contained (published) in the insolvency register. This interpretation, however, makes the redaction only formal, as usually a natural person's personal data can be obtained from other documents published in the insolvency register.

The inspection further states that as the receivables of creditors and the amount of such receivables are the subject of insolvency proceedings connected to settlement proceedings in accordance with Section 2(a) of Act No. 182/2006 Coll., the redaction of such data would thwart the legislator's intent. Declaring receivables is a procedural act by which a creditor exercises the satisfaction of his rights in insolvency proceedings. The details of the application are set out in Section 21 of Decree 311/2007 Coll. In the event that the creditor submits an application, it is again only the court that can decide on the redaction of the data according to Section 422(1) of Act No. 182/2006. The Office is then not authorised to review the court's decision on redaction. In the case where a complainant objected to the publication of the creditor's receivable that was the subject of the insolvency proceedings (in the case at hand, the natural person's funds on a specific account belonging to the bankrupt party), the inspectors were convinced by the courts that the amount of the receivable and the legal grounds of the insolvency proceedings and the right of the parties to the proceedings to contest the receivable claimed by the creditor, e.g., as regards the amount and legal grounds, including the debtor's account number, cannot be redacted and, because of this fact, disclosure of personal data did not take place at variance with Act No. 101/2000 Coll.

The inspection found that data pertaining to other parties is not always redacted in documents published in the insolvency register in accordance with Section 422(2) of Act No. 182/2006 Coll. The conclusion of the inspection protocol thus stated a breach of Act No. 101/2000 Coll. It should, however, be stated that under the mentioned provision, an absurd situation comes about where the court has to redact data in published documents even though such data is available in public registers (Trade Licence Register, Commercial Register, etc.); nevertheless, from the point of view of the obligations imposed on the data controller (the respective court), the provisions of Act No. 101/2000 Coll. have been breached.

It can be stated based on assessment of the ascertained facts that the inspected entities did not process (collect) the personal data of natural persons in insolvency proceedings in a scope that would go above and beyond what is stipulated in Act No. 182/2006 Coll.

With regard to the legal assessment of the facts ascertained by the inspections, the issue of publication (disclosure) of personal data and their redaction in the insolvency register will be discussed with the Ministry of Justice, as there are ambiguities in interpretation of the process and problems with implementing it in practice.

### Inspection of the processing of personal data of motor vehicle owners and operators in the AUTOTRACER system (VIN processing)

The subject of the inspection commenced at Cebia, spol. s r.o. (the "Company") in February 2014 at the instigation of the President of the Office was observance of the data controller's/processor's obligations when processing the personal data of owners and operators of vehicles in connection with the operation of the AUTOTRACER system, with a focus on observance of the obligations under Article 5(2), Article 5(4), Article 11(1) and Article 13 of Act No. 101/2000 Coll.

The company operating the AUTOTRACER does business in the area of verifying the origin and history of used vehicles. The AUTOTRACER information system was created five years ago as an on-line information system that provides immediate assistance to anyone buying a used car.

According to the inspectors' findings, about 90% of the system database comprises the following data: VIN (Vehicle Information Number), status of the odometer, and the date when the status of the odometer was recorded (the so-called data "trio"). The system also contains an overview of the material used for repairs and an overview of repair work carried out on the vehicle in question. This data is obtained from brand name and non-brand name services stations (approx. 750). Most files contain three columns: The VIN of the vehicle, status of the odometer and the date when the respective odometer status was recorded. The company does not guarantee the information contained in the system. About 20 errors per month are discovered in the system. The Company removes such errors. Only the mentioned trio is stored in the AUTOTRACER database. Information about the source of the data is not recorded in the database, so it cannot be found out retrospectively. The data is provided by brand name and non-brand name service shops based on a signed agreement between the respective service shop and the Company. In the case of brand name service shops, the terms and conditions of cooperation with the importer or manufacturer are agreed before cooperation with the brand concerned (Škoda - enters the same scope of information into the electronic service book stored in the central database; the vehicle owner can request a copy at an authorised service shop; VW importer, Honda, Mitsubishi, Toyota – provide the same information that is available to the public on their respective websites).

In the AUTOTRACER system, the company records about 120,000 queries per month not only from domestic clients/customers, but also from foreign clients/customers, namely from Eastern Europe, where vehicles from the Czech Republic are exported to. Not only ordinary clients/customers, but also used car dealerships and the public authorities (Police of the Czech Republic, tax offices etc.) use the system. The AUTOTRACER System provides the same information to both ordinary clients/customers as well as to contractual partners and the public authorities. The AUTOTRACER system is used by many public authorities, which use the data in the system for their day-to-day work.

The AUTOTRACER system further makes use of insurance company data based on agreements concluded with Global Expert, s. r. o., and UNIQUA pojišťovna, a.s. (structure of data: VIN, vehicle damage calculation, description of damage, enumerated damage); own system for ascertaining the real year of manufacture of the vehicle: from the VIN code; publicly available data from the websites of vehicle manufactures that serve as service support (structure of data: technical data about the vehicle, i.e., brand, model, type of motor etc.); publicly available information from the websites of leasing companies in the Czech Republic (approx. 24), in the Slovak Republic via the Association of Leasing Companies (in both cases only yes/no to the question of whether financed or not). The status is ascertained on-line at the moment the system is queried; information is not stored further in the system. The server makes use of publicly available data from the Czech Ministry of the Interior and the Slovak Ministry of the Interior; the data is not collected in the system, however. The unique ICARIS system is also used. This means that data for identifying a vehicle – general information on how to identify a vehicle and how to verify the merits of its identifiers (VIN stamp, serial number plate etc.) – is

used. Data from abroad, specifically from companies operating portals aimed at the sale of scrap vehicles are also used to verify origin of a vehicle. This is done also based on agreements concluded with such companies.

According to the inspectors' findings, the AUTOTRACER system does not contain vehicle registration numbers or the personal details of former or current owners or operators of the vehicles.

VIN is a number/code that usually is composed of 17 digits (letters and numbers). The meaning of each digit is as follows:

- 1st digit – code of the country where the vehicle was manufactured
- 2nd digit – specifies the manufacturer (brand) of the vehicle
- 3rd digit – specified the type of vehicle or manufacturing division
- 4th to 8th digit – VDS (Vehicle Descriptor Section) - attributes of the vehicle (engine, model, series etc.) encoded specifically by the manufacturer
- 9th digit – control number
- 10th digit – production year
- 11th digit – assembly plant code
- 12 - 17th digit – serial (manufacturing) number of the vehicle, unique for the manufacturer and assembly plant

The VIN is thus data about the vehicle that accompanies the vehicle throughout its "life cycle". This is a kind of "personal identification number" of the vehicle - an identifier that does not change, unlike the vehicle registration number, which is created and changed in compliance with international legislation and is always allocated to a specific vehicle and the specific owner of the vehicle. Processing the VIN in conjunction with the registration number of the vehicle or data about the vehicle owner may be deemed personal data processing under certain circumstances according to Act No. 101/2000. Data about the vehicle registration number is not collected by AUTOTRACER and without this information it is not possible to identify the vehicle owner or operator (natural person) only based on the VIN. The controlling inspector concluded in the inspection protocol that Cebia, spol. s r.o. does not collect or process personal data under Act No. 101/2000 Coll.

During the above inspection, the Office received an instigation that was aimed against publication of information about vehicles with odometers that had allegedly been tampered with on [www.sdruzeni-sova.cz](http://www.sdruzeni-sova.cz), on the grounds that the case at hand concerns the disclosure of information related to a specific vehicle where in some cases data about the vehicle owner or operator is published as well. The Office stated that the data published by the Sdružením na ochranu vlastníků automobilů - SOVA, o.s. (Association for the Protection of Automobile Owners - the "Association") pertains to specific automobiles. It is true that based on such data, especially the use of the VIN code using an internet search engine, it is usually possible to find the source advertisement which, if the vehicle is sold by a natural person, also contains contact data (name, telephone or e-mail address) that such person posted on the internet for the purpose of selling the vehicle in question. At least in the case of automobiles sold by a natural persons, the matter can be one of personal data processing according to the definition under Article 4(a) of Act No. 101/2000 in accordance with Article 2(a) and Recital 26 of Directive 95/46/EC of the European Parliament and of the Council. This data, together with information about sellers and legal persons, is collected without further differentiation, compared and



disclosed by the Association. Although the Association clearly aims not to identify specific natural persons (individuals) but only to process data about some automobiles being sold, the Association has to be aware that even personal data about the sellers/natural persons (individuals) is being processed along with the data that is being processed to this end. For this reason, at least in the case of the information published about automobiles that are being sold by natural persons (individuals) at the given time, personal data processing is formally taking place according to the legal definition of this term. The aim of work carried out by the Association, as declared by it and by the findings from the previous inspection by the Office, is to publish information about automobiles that are being sold and where it is suspected that inaccurate information is being given about the technical state of the vehicle, especially about the odometer reading.

The purpose of such data processing can generally be deemed legitimate and legal, which it is even if such processing is deemed personal data processing, provided the conditions imposed by Czech and European legislation for personal data processing are met. Another condition that has to be met for personal data processing to be legal is the existence of legal grounds, i.e., reasons for personal data processing anticipated by the law. It was stated in the instigation that the Association clearly does not have consent from the seller to use their personal data further. According to the Office, consent is only one of a number of legal grounds for processing data. The grounds that can be applied to the Association's activities are set out in Article 5(2)(d) and (e) of Act No. 101/2000 Coll. According to the former, it is possible to process personal data without the affected person's consent if it is legitimately disclosed personal data. The latter then allows personal data processing in the situation where such processing is necessary to protect the rights and the legally protected interests of data controller, data recipient or other affected person, who in this case may be a potential buyer or party interest in purchasing the vehicle in question and where it is suspected that false technical data is being provided. Even though the Association's activities have been assessed as personal data processing, such processing would be possible without the consent of the persons in question based on the above legal grounds. The Association is also not suspected of breaching other obligations under Act No. 101/2000 Coll. The Office also stated that should a seller, be it a legal or natural person, believe that they incurred damage from that the activities of the Association, especially by the fact that their automobiles were designated as a vehicle with a tampered odometer, it is necessary to claim such damage through civil law options, as the Office does not have the power to decide on such disputes. As mentioned above, the Office believes that protecting rights and legally protected interests by publishing information about automobiles that are being sold and where there is reason to suspect that false technical data is being provided is legitimate grounds. With regard to this fact and the principle of ultima ratio, according to which it is necessary to apply means available under public law, e.g., an inspection or administrative proceedings, only if a remedy is unavailable under private law or (for the protection of rights) civil law, the Office will not, in this case, intervene in the relationships between the sellers and other entities.

## III. INSPECTIONS ACCORDING TO VARIOUS THEMATIC GROUPS

### A. Personal data processing via monitoring systems at places of work, in means of transport and in residential buildings

#### Camera surveillance systems in residential buildings

In July 2014, the Office received an instigation from the association of buildings owners in Kolín (the "Association") to conduct an inspection of the Kolín Construction Housing Cooperative (the "Cooperative") in the matter of the operation of a camera surveillance system in residential buildings due to a suspected breach of Article 5 and Article 10 of Act No. 101/2000 Coll. It ensued from the instigation that the Association was established in December 2013 based on the law. After the election of the bodies took place in March 2014, the Association also assumed management of the building. A part of the assumption of management of the residential buildings from the Cooperative was the camera surveillance system, from which the Association allegedly did not obtain, despite oral and written requests, the supporting administrative documents that would allow its due operation. According to the Association, the Cooperative handed over insufficient documents in June 2013, as it did not provide all informed consents from the subjects in question in connection with the operation of the camera surveillance system installed in the residential buildings regarding monitoring of the lifts. Furthermore, the Company allegedly received an invalid signature sheet, as it had not been updated. The contested discrepancy between the actually operated camera surveillance system and legislation was not remedied by the Cooperative at the Association's request. For this reason, the Association believed that it could not re-register at the Office and claimed that the camera surveillance system continued to be illegally operated and managed by a foreign subject without the Association's consent. Based on the above, the Association submitted an instigation for an inspection of the former owner (Cooperative) in connection with the camera surveillance system operating in a specific residential building in Kolín. As part of the tasks undertaken prior to commencement of the inspection pursuant to Section 3 of Act No. 255/2012 Coll., on inspections (the Inspection Code), the inspector discovered that the Association took over the respective camera surveillance system from the Cooperative on the day that the building management agreement expired or, more precisely, after the constitutive meeting of the Association; furthermore, it took over the keys from the common areas of the building from the former chairman. The Cooperative thus ceased being the manager of the building in question at the end of April 2013.

Based on the inspection, the responsible inspector stated that on the date that the Association assumed management of the building from the Cooperative, the Cooperative relinquished all of obligations and commitments ensuing from the position of personal data controller with regard to the camera surveillance system in question and the Association took over all of the ownership rights even with regard to the operated camera system, which fact was corroborated by the minutes of the constitutive meeting of the Association. Thus, the Association became the actual owner of the camera surveillance system upon assuming ownership of the



installed camera system, thus also becoming the personal data controlled under Act No. 101/2000 Coll. As of such moment, the Association thus become the sole entity responsible for its lawful operation and in accordance with Article 5(4) of Act No. 101/2000, it was and is obliged to demonstrate the consent of the data subjects with processing personal data for the entire processing period. Thus, if the complainant objected to the unlawful operation of the camera surveillance system, it was his obligation to terminate the processing of the personal data via the camera surveillance system in the residential buildings at the moment when it took over the camera surveillance system from the Cooperative or to bring this activity in line with the law. The statutory registration obligation and the related obligation in accordance with Article 5(4) of Act No. 101/2000 Coll. to demonstrate the data subjects' consent with the processing of their personal data passed on to the complainant, which should have remedied any shortcomings in the documentation, disconnected the contested camera surveillance system in the lift and register with the Office anew no later than by the day following the takeover of the building from the Cooperative.

In compliance with Section 3 of Act No. 255/2012, the Association was sent a warning about a possible breach of Act No. 101/2000 Coll. and a request to bring personal data processing in line with Act No. 101/2000 Coll., including the change in registration at the Office, which will bring the situation in line with Act No. 101/2000 Coll., and if the required steps are taken, the instigation will be adjourned. The Association was also imposed the obligation to provide ongoing information to the Office inspector by the stipulated deadline. The complainant subsequently registered the camera surveillance system at the Office anew and informed the Office inspector of such fact. The Cooperative also requested termination of its registration. Based on the above, as both parties remedied the situation and brought the state of affairs in line with Act No. 101/2000 Coll., the instigation was adjourned.

### **Camera surveillance systems in public transit**

On 19 June 2013, Brno Public Transit Company (Dopravní podnik Města Brna –“DPMB”) informed the office that it was to process the personal data of passengers. The Office decided to commence administrative proceedings as it had warranted concerns that the provisions of Article 5(1)(e)(2) of Act No. 101/2000 Coll. were being breached. During the course of the administrative proceedings, the Office decided to suspend the proceedings pursuant Article 17(2) of Act No. 101/2000 as it was discovered that the participant in the proceedings was not breaching any of the conditions set out in Act No. 101/2000 Coll. In the administrative proceedings, DPMB submitted and documented previously adopted measures that did not lead to rectification and minimisation of the damage inflicted in mass transit vehicles and these less invasive procedures were not successfully eliminating or at last reducing damage.

The Office examined especially thoroughly the intention behind personal data processing without the consent of data subjects and whether such processing was not in fact at variance with the right of the data subjects to protect their privacy and personal life. It based its approach in particularly on the party's declared facts, especially the amount of the mentioned damage, which the deployed camera surveillance system should minimise, and from the measures that the party adopted prior to opting for the camera surveillance system. This concerned a combination of HR, technical and other preventive measures that should have served to prevent the perpetration of damage inside trams and protect both tram passengers and drivers.

The placement of the cameras showed that only the inside of the tram would be monitored and that the driver's cabin would not be. The installation of a camera surveillance system with a recording function in the tram cars can be considered adequate with regard to the declared purpose and with regard to the means and measures used prior to the implementation of the system.

The administrative body took into account the fact that the party to the proceedings placed great emphasis on fulfilling its obligations under Article 13 of Act No. 101/2000 Coll. It minimised as much as possible access to the recordings made by the camera system, with the sole recipient being the criminal authorities. Each export of data will be subject to a thorough review as to its necessity. The party to the proceedings drew up an entire series of organisational, technical, HR and administrative measures to safeguard personal data. It also stipulated the method used to check the observance of these measures and the process for assessing the effectiveness of the deployed camera surveillance system.

In the administrative proceedings, the party had registered the processing of the personal data of public transit passengers using a camera surveillance system with a recording function in 29 Škoda 13T trams.

A review of the facts stated by DPMB in the notification of processing (change of processing) of the personal data of passengers and the facts ascertained by the Administrative Operations Department via administrative proceedings under Article 17 of Act No. 101/2000 Coll. and the fulfilment of the obligations of a data controller were the reasons for including the inspection of DPMB in the Office's supervisory plan for 2014. The inspection was commenced on 15 January 2014.

The installation and operation of a camera surveillance system was considered by DPMB especially because of the marked financial costs expended on fixing the damage caused to public transit vehicles, i.e., to urgently protect in particular the substantial property owned by the data controller. Another related measure was the possibility to document violent crime perpetrated against passengers or against the employees of the inspected entity. This will have a substantial preventive effect on potential criminals and vandals, as objective and public information will be available about the fact that perpetrators will be caught and forced to pay damage compensation caused by their crime.

In connection with the processing of personal data of passengers and employees, the inspection did not discover any breach of Act No. 101/2000 Coll. DPMB adopted personal data protection principles in connection with the operation of the camera surveillance system with recording equipment located in public transit vehicles. Physical security, including the logging and export of data, was examined. DPMB fulfilled the duty to inform under Section 11 and adopted the necessary measures under Article 13(1) and (4) of Act No. 11/2000 Coll. Making a camera recording pursuant to Article 5(2)(e) of Act No. 101/2000 Coll., i.e., without the data subjects' consent, is possible only if it is the property of the inspected entity that is being monitored, the legitimate interests of the data subjects/passengers/employees are protected (protection of their property and health) and past measures had not be sufficient. In the case at hand, with regard to the monitoring of activities inside public transit vehicles, the amount of damage caused to public transit vehicles, the need to secure and protect the property of passengers and ensure the safety of DPMB employees, it was stated that the mentioned personal data processing is not at variance with Article 5(2)(e) of Act No. 101/2000 Coll. The period for storing records does not

allow for the regular monitoring of data subjects who are informed about the scope of monitoring. The measures under Article 13 of Act No. 101/2000 Coll., including minimisation of access to recordings, ensure that personal data is processed for the stipulated reason without infringing on privacy, which would not be appropriate for this purpose. The inspection did not find that the collection of personal data would be at variance with Section 316(2) of the Labour Code. The operation of the camera system then corresponds to the facts ascertained as part of registration proceedings and the follow-up proceedings under Article 17 of Act No. 101/2000 Coll.

With regard to the introduction of the DPMB camera surveillance system in public transit vehicles, the Office will assess whether it continues to be necessary and is reasonable in scope; therefore an evaluation report for the first half of 2014 was requested as the basis for assessing whether the conditions for the continued operation of the camera system continue to exist. The DPMB thus sent the office an evaluation of the effectiveness of the recordings made using the camera systems located in the trams for the first half of 2014.

## B. Processing sensitive data in connection with the provision of health care services

### **Loss of a patient's medical file in Lužice Hospital**

The Office's inspector conducted an inspection from September 2012 to March 2013, the subject of which was observance of the data controller's obligations under Act No. 101/2000 Coll. with a focus on processing the personal data of patients of the health care facility Lužické nemocnice a polikliniky, a. s. (the "Hospital") and the related inspection of medical records according to Article 13 of Act No. 101/2000 Coll.

The complaint was sent to the Office by one of the Hospital's patients (the "Complainant"), who called attention to the alleged loss of her medical records, which claim she backed with a document drawn up by the appropriate body of the Czech Medical Chamber (Česká lékařská komora - "ČKL") in Děčín, with which she filed a complaint concerning the medical care provided to her in June 2009. In the document, ČKL stated that it was impossible for them to find her medical records and used this as the grounds to initiate disciplinary proceedings in the matter of the provision of proper care during her hospitalisations in 2009.

From the findings obtained during the inspection based on the requested records and documents, the facts were ascertained and a legal assessment of the case was performed with regard to the how the Complainant's medical records were handled and with regard to the current situation, especially from the point of view of observance of the obligations of the Hospital, as the controller of the personal data maintained in the medical records, under Article 13(1) of Act No. 101/2000 Coll. It was discovered that the Hospital lost part of the Complainant's medical records maintained in paper form, a fact that the Hospital admitted, and the medical records kept in electronic form were incomplete. At the time when the Complainant's medical records were lost, the Hospital did not have measures in place to prevent the loss of medical records, by which it breached Article 13(1) of Act No. 101/2000 Coll. At the same time, the Hospital breached Article 13(2) of Act No. 101/2000 Coll. as at the time when the loss of the Complainant's medical records occurred, it did not have technical and organisational measures in place to safeguard personal data.

When assessing the current situation, it was also found that the measures that have been adopted are still insufficient. The portable filing room and the central filing room were not sufficiently secured and no internal regulations were in place to prevent the possibility of the loss of medical records; therefore, the Hospital breached Article 13(1) of Act No. 101/2000 Coll. Furthermore, the Hospital did not create electronic records that would allow it to determine and verify when the electronic medical records were reviewed, by whom and for what reason; therefore, the Hospital breached Article 13(4)(c) of Act No. 101/2000 Coll., i.e., the Hospital is unable to ensure on an ongoing basis that access to the Hospital Information System is authorised through random checks.

The Complainant filed a complaint with ČKL and requested an assessment of the medical care provided to her at the gynaecological-obstetrics department of the Hospital, which, according to her, failed to discover the threat to her foetus during her hospitalisation, which resulted in her giving birth to a dead foetus. The regional association of ČKL in Děčín conducted a repeated investigation, the outcome of which was a decision by the Review Committee not to commence disciplinary proceedings. The decision states that “even though it is not possible to find in the medical records provided to us any evidence that the approach taken by the physicians was erroneous, and the death of a foetus in a substantial percentage of cases occurs unexpectedly and without a clear explanation, without access to complete documentation it is not possible to make a responsible and objective decision in the case. The Review Committee even requested the regional perinatologist for an assessment of the case, but he refused to perform the assessment without documentation.” The Děčín ČKL Review Committee stated that “in the case at hand, it is issuing a new decision not to commence disciplinary proceedings for the reason that it was not possible to prove the guilt of any of the accused physicians.”

The Complainant did not file a criminal complaint with the Police of the Czech Republic until 2012 about the loss of her medical records and neglected care by the Hospital. The Police of the Czech Republic informed the Office that the case concerning the suspected crime of harm to health under Section 244(1) of the Criminal Code, a crime that an unknown perpetrator was to have committed, is being suspended as the investigation failed to prove that a crime was perpetrated by a specific person. At the same time, it ensued from the decision of the Police of the Czech Republic that the Police of the Czech Republic had an expert opinion drawn up by an expert in the field of gynaecology and obstetrics, who stated that he “only received incomplete documentation from the Hospital to a duly filed request with information that some of the records were lost; due to this fact, it is not possible to reputably respond to the questions posed, opine on and assess the circumstances that lead to the death of the foetus.” At the same time, the expert stated the following: “The fact that in the event of an unsuccessful conclusion of medical efforts it suffices to lose the relevant documents to bring about the conclusion of ‘if there is no evidence it is not possible to bring charges’ is highly disconcerting in this case!” The expert further added that he is worried that the loss of medical records could become a “national pastime”.

The Office has identified with the expert’s opinion and expressed concern about such cases reoccurring. For this reason it focused its supervisory activity on the way medical records are handled in health care facilities, with an emphasis on the fulfilment of the obligations under Article 13 of Act No. 101/2000 Coll. In 2014, the health care facility Lužická nemocnici s poliklinikou, a. s. was imposed a fine of CZK 120 000 as part of administrative proceedings.

At the same time, the Office could not leave without notice the actions of ČKL, which not only failed to report the loss of the medical records to the relevant authority, i.e., the Office, but by its tardiness also caused the administrative offence of loss of a part of specific medical records to become statute-barred, thus preventing the Hospital, as the personal data controller, from being punished for breaching its obligations. For this reason, the Office conducted an inspection of the way personal data is processed at ČKL as part of its procedure for handling complaints filed against physicians.

#### **Content of data in a medical evaluation**

The Office obtained a complaint concerning a physician who according to the complainant was asked by an officer of the Labour Office of the Czech Republic for an evaluation of his state of health. According to the complainant, the physician drew up and submitted a medical evaluation of his state of health in connection with his application for job rehabilitation at the Labour Office of the Czech Republic. According to him, the physician gave information about his state of health and the state of health of his closest family members to a third party, i.e., an officer of the Labour Office of the Czech Republic, without his consent and by doing so she, in his opinion, grossly breached the code of medical ethics and, at the same time, acted unlawfully.

According to the Office's inspector's findings, the physician, when drawing up and passing on the medical evaluation, acted in compliance with Section 9(1) of Act No. 453/2004 Coll., on employment, Act No. 373/2011 Coll., on specific health care services, and Act No. 372/2011 Coll., and health care services and the conditions for providing them. The complainant, however, demanded a review of the content and scope of the evaluation of his medical state. In the case at hand, the Office's inspector called attention to the standpoint issued by the Ministry of Health which the Office obtained in connection with a different inspection and which pertained to the content of medical records. In the respective case, the Office had requested the Ministry of Health to respond to question of which competent supervisory authority is authorised to conduct oversight in the area in question.

The Ministry of Health sent the Office its standpoint on the question of designation of the competent supervisory authority to oversee the maintenance of medical records and, inter alia, informed the Office that Act No. 372/2011 Coll. does not specify any single supervisory authority as being responsible for overseeing only the maintenance of medical records and, as such, such sole authority is also not the Office for Personal Data Protection.

Based on the above standpoint, the Office's inspector stated that the Office did not have the power to assess the content and scope of the medical evaluation issued by the physician at the request of the Labour Office of the Czech Republic, as the Office does not have the power to conduct inspections in the area of personal data processing in terms of legitimacy and completeness of records in connection with the provision of health care. For this reason, the complaint was dismissed.

#### **Processing of personal data of the clients of a health insurance company during their pre-registration**

The Office's inspector conducted a inspection of the Military Health Insurance Company of the Czech Republic (Vojenské zdravotní pojišťovna České republiky - "VoZP ČR"), the subject of

which was observance of the obligations imposed on data controllers by Act No. 11/2000 Coll., with a focus on the processing of the personal data of VOZP ČR clients in connection with their registration. The inspection was carried out based on complaints filed by 22 data subjects, the merits of which was the fact that the complainants' personal data was used for their wrongful registration at VoZP ČR without their consent.

The inspection showed that the wrongful registration of the data subject at VoZP did in fact take place without their knowledge based on brokerage activities taking place based on a non-exclusive sales representation agreement concluded by and between VoZP ČR with a natural person not registered in the Commercial Register and doing business under the Trade Licensing Act. The mentioned natural person was carrying out contractual activities via approx. 200 "recruiters". The inspection found that the Insurance Applications and Personal Files of the insurance company were not drawn up in the presence of the affected persons (complainants). The inspector stated that VoZP ČR did not have sufficient mechanisms in place in connection with the pre-registration of policy holders via the sales representatives to detect the submission of "fictitious" Insurance Applications and Personal Files of the health insurance company. With regard to the agreement concluded with the natural person with the aim of acquiring new clients (policy holders), VoZP ČR should have set up already at the time of concluding the agreement internal rules for verifying the data indicated in the Insurance Application and Personal Files of the health insurance company submitted by the sales representatives, together with a nominal list of the individuals selling the Insurance Applications, not to mention the pre-registration application, still prior to executing the registration itself.

The inspector did not dispute the obligation to register policy holders in accordance with Act No. 48/1997 Coll., on public health insurance, but did state that the personal data controller, i.e., VoZP ČR in this case, is obliged under Article 5(1)(c) of Act No. 101/2000 Coll. to process accurate personal data. As VoZP ČR demonstrably processed inaccurate person data based on "fictitious" Insurance Applications and Personal Files of the health insurance company, which documents were submitted to it by sales representatives, it, being the controller of the personal data of its clients, breached Article 5(1)(c) of Act No. 101/2000 Coll.

VoZP ČR failed to make sure that the adopted technical-organisational measures of the sale representatives, as the personal data processor, correspond to the personal data protection requirements defined in Article 13 of Act No. 101/2000 Coll.

VoZP ČR was then imposed a fine of CZK 70 000 during administrative proceedings for breach of the obligations set out in Article 5(1)(c) of Act No. 101/2000 Coll.

## C. PERSONAL DATA PROCESSING IN REGISTRIES OF DEBTORS

### Personal data processing on [www.dluzis.cz](http://www.dluzis.cz) and in the SOLUS debtor registries

1.

In 2014, the Office's inspector conducted an inspection of the non-banking registry of debtors based on complaints from citizens. The issue concerned in particular the processing, accessing and disclosure of personal data in connection with information about clients defaulting on alleged debts to various companies. The related inspections took place at companies providing non-banking credit services, leasing companies and telephone operators entering information



about client defaults into the respective debtor registries. An inspection of two debtor registry operators also took place. A total of seven related inspections took place.

The common denominator of almost all of the findings was the absence of the legal grounds for processing personal data in the registries of debtors, the outcome of which was a breach of the obligations set out in Article 5(2) of Act No. 101/2000 Coll., i.e., the obligation to process personal data only with the consent of the data subject, as no exemption exists under the law for the processing of personal data in debtor registries.

One of the inspected entities was a natural person doing business under the Trade Licensing Act and operating a debtor registry under the website [www.dluzis.cz](http://www.dluzis.cz), where it publishes the names and addresses of alleged debtors and provides an unlimited group of people with access to personal data. The inspected entity operates the internet application "Dlužíš.cz", the aim of which is to allow creditors to publish advertisements on the website, for a fee, for the purpose of finding other creditors for filing insolvency proposals against a specific debtor. Another reason why creditors are interested in the publication of the identity of a debtor and information about their debts is pressure on the debtor to pay their debts. "Dlužíš.cz" is intended for all creditors who have an unpaid invoice past due. Registration of a creditor according to the general business terms and conditions is, once the basic conditions are met, made possible free of charge, with the option to notify a debtor about their entry in the debtor registry. The legal grounds for personal data processing were stipulated by the inspected entity as the express consent of the debtor with such publication. Debtors are always charged 2-6% of their stipulated debt as the fee for being removed from the register. The website of the "Dlužíš.cz" is operated for the purpose of the business activities of the inspected entity.

The inspection found that the following information is made available about the debtor: name, surname, registration number, address (street, house number, town, and post code). The following information about the respective creditor is also available: name, registered office or place of business, identification number, bank account, variable code, description of receivable (e.g., invoice for services rendered - connection to internet), invoice number, days past due, amount owing and penalty amount. At the same time, the list of debtors contains information about the name/surname of creditors. If the creditor is a natural person doing business, information about them appears in the following scope: name, surname, identification number, registered office or place of business. The inspection showed that the inspected entity did not have the consent of a single data subject, i.e., the inspected entity disclosed personal data on [www.dluzis.cz](http://www.dluzis.cz) without legal grounds at variance with Act No. 101/2000 Coll. Based on the inspection findings, the inspected entity was ordered to adopt remedial measures and, in the framework of the related administrative proceedings, was fined CZK 19,000 for committing an offence.

2.

Another inspected entity at which a repeat inspection occurred was the SOLUS, interest association of legal persons (Zájmové sdružení právnických osob SOLUS - "SOLUS"), which maintains the so-called negative registry of debtors. Many complaints were filed against this company by people convinced that they were listed wrongfully in the negative register of natural persons. A part of the subject of the inspection was the fact that SOLUS continues not

to respect the final decision of the Office that was issued based on previous findings, and refuses to change its approach to processing the personal data of the clients of its member companies.

An illustration of the issue that the Office's inspector addresses in the case of the inspection of the processing of personal data in the negative register operated by SOLUS is the inspection that was concluded with an inspection protocol that showed that the inspected entity had processed the personal data of complainant J.R. in the negative register to the following extent: name, surname, personal identification number, full address, amount owing past due, date when the default arose, date of registration in the information system, date of settlement of the outstanding amount, date of the last change and the name of the creditor. This data was processed based on the consent provided by J.R. when concluding a personal loan at Raiffeisenbank a.s. As he defaulted on his loan, his personal data was handed over to the inspected entity on 3 July 2009. J.R. was in default until 26 October 2009, when he paid off his debt (based on the terms and conditions of SOLUS, the data should have been deleted after three years, i.e., as at 26 October 2012). On 16 November 2011, J.R., sent to his bank (Raiffeisenbank a. s.) a notice revoking his consent to his personal data being processed, including a statement that he does not agree with his personal data being processed in the negative register operated by SOLUS. The bank did not satisfy his request.

On 20 February 2012, another complainant (R.L.) expressed via e-mail his disagreement with the processing of his personal data in the negative register operated by SOLUS and requested that his name, surname, personal identification number, date of birth and address be deleted. The mentioned personal data was being processing based on an agreement concluded by and between R.L and Home Credit a.s. The receivables arising under this agreement had still not been paid up at such time. Answering on behalf the inspected entity was Společnost pro informační databáze, a.s., which stated the SOLUS members are the source of information about clients and that only association members are authorised to process the information and do so with the express consent of the person in question. It further stated that it was found that Home Credit, a.s. entered his personal data into the register of natural persons in compliance with the Rules for Creating, Managing and Utilising Databases of Consumers in Default applicable to association members based on the demonstrable consent to personal data processing in the case of a breach of the contractual relationship and upon meeting the criteria for inclusion in the register. R.L. turned to Home Credit a.s. with the same request on 20 February 2012. Home Credit a.s. responded that its records show an unpaid receivable and that his personal data are being processing in compliance and under the conditions of the granted consent, including the conditions for revoking such consent. As the debt had not been settled, the revocation of consent to personal data processing is thus invalid. The indicated records are also in compliance with the company's statutory obligations regarding responsible lending.

The inspector assessed these finding as follows: the inspected entity is clearly processing the personal data of J.R. and R.L. in accordance with Article 4(a) and (e) of Act No. 101/2000 Coll. This data is collected in the negative register operated by SOLUS, whereas the inspected entity decided on the purpose and means of processing, is doing the processing and is responsible for it. As such, it is the personal data controller in accordance with Article 4(j) of Act No. 101/2000 Coll.

Both J.R. and I.L. granted consent to processing personal data when concluding the respective agreements with Raiffeisenbank a.s. or Home Credit a.s. The purpose of the personal data



processing included the handover of information on breach of contractual obligations, including the scope and nature of such breach, to the inspected entity. The handover of personal data to the inspected entity thus took place in accordance with Article 5(2) of Act No. 101/2000 Coll.

However, the inspection also found that in two cases the SOLUS register processed the personal data of individuals who never concluded any agreement with SOLUS, as the association was at fault of collecting inaccurate personal data (one case had to do with a stolen identity; in the other case an incorrectly concluded agreement based on the incorrect identification of a client), with SOLUS refusing even in this case to delete the personal data of these individuals. Both complainants discovered that they were recorded in the SOLUS register when their mortgage applications were rejected for the reason that they were registered as debtors.

In another case, SOLUS was processing the personal data of data subjects that concluded an agreement at the time when the contractual company was not a member SOLUS, i.e., that the debt arose when the company was not a SOLUS member. The debt that the member company was owned amounted to CZK 139 and arose in 2004.

In two cases, a request of the complainants to delete the entry in the SOLUS register was rejected, even though the matter concerned individuals that only requested the conclusion of a non-banking agreement and not even one of the member companies concluded an agreement with the complainants. In such case, SOLUS took it upon itself to make decisions that pertain to a banking register. In one case it was found that SOLUS refused to delete personal data even after the deadline that it itself had stipulated as the data retention period, i.e., three years after the complainant settled his debt.

The revocation of consent to personal data processing sent by J.R. to the inspected entity or, more precisely, the rejection thereof by the inspected entity resulted in the state where the inspected entity processed such personal data at variance with Article 5(2) of Act No. 101/2000 Coll. At the same time, it is the inspector's opinion that inspected entity breached its obligations ensuing from Section 10/2000 Coll., as by its actions did not safeguard the data subject from wrongful infringement of his or her privacy and personal life.

The Office's inspector stated that processing personal data for the purpose of informing the inspected entity's members of breaches of contractual obligations is processing that does not fall under any of the exemptions set out in Article 5(2)(a) through (g) of Act No. 101/2000; this obligation does not ensue from any legal regulation, is not necessary for the performance of the agreement which the data subject and the inspected entity are parties to, or for the performance of the agreement between the data subject and the inspected entity's member.

The Office's inspector further stated under Article 4(n) of Act No. 101/2000 Coll., consent is free and conscious show of will, with the content thereof being the data subject's permission to have personal data processed; it is thus a unilateral legal act and not an agreement between the data controller and the data subject. Consent with processing personal data is therefore not required for the conclusion of the respective agreement with the companies providing credit products and services and is provided above and beyond the contractual relationship itself. It is thus only up to the data subject to grant consent or not to grant consent and, at the same time, when and if he or she revokes such consent. The data controller has to respect such revocation. Such revocation results not only in the termination of personal data processing under Article 5(2) of Act No. 101/2000 Coll. but also the obligation under Article 20(1) of the same to delete such data.

In the Office's legal opinion, it is possible to process the personal data of clients/natural persons for the purpose of the mutual exchange of information between creditors only with the consent of such clients/natural persons. Processing (i.e., especially placing and updating) information in non-banking registers in the case of clients-natural persons is subject to the provision of consent with personal data processing. Act No. 101/2000 Coll. allows people to revoke their consent at any time to the processing of their personal data. If legislators did not address the activities of operators of non-banking registries of debtors (as opposed to banking registers) in a special law, such registry operators have to observe general legal regulations, i.e., Act No. 101/2000 Coll.

SOLUS does not agree with this legal opinion and on 12 February 2013 turned to the Municipal Court in Prague to contest the Office's decision.

The inspection found that SOLUS as a whole, i.e., its offices as well as its processing company Společnost pro informační databáze, a. s. and the various members of the association, do not have a common methodology and procedure in place to handle complaints filed by data subjects as part of the data subjects' access to information and when handling requests as part of the protection of the data subject's rights and the deletion of personal data. The absence of rules results in an unsystematic and differing decision-making process observed by SOLUS and by the various member companies when handling identical requests from clients.

The inspection found that SOLUS or its members in the framework of their business terms and conditions obtain consent with the processing of personal data in the SOLUS registries but provide different information about the right to revoke consent or about processing periods in the SOLUS registries. In the last quarter of 2014, the Office began addressing other complaints of unauthorised personal data processing by SOLUS.

With regard to this issue, it should be stated that the Office, when applying Act No. 101/2000 Coll., has no interest in protecting individuals who do not fulfil their obligations as debtors to creditors, i.e., to protect people that do not fulfil their obligations, but to protect people whose personal data are being processed without legal grounds, which results in an infringement of their privacy and personal lives.

## D. ENERGY SERVICE PROVIDERS AND THE PROCESSING OF CLIENT'S PERSONAL DATA

### **Observance of the obligation of personal data processors with focus on the data subjects' consent when concluding agreements through general business terms and conditions**

The inspection was aimed at companies with activities regulated by a special law.

Three entities were inspected: RWE Energie, s.r.o., ČEZ Prodej, s.r.o., and O2 Czech Republic a.s. The inspection of RWE energie, s.r.o. already commenced in 2013 and was completed in 2014. According to Office's inspector, as RWE Energie, s.r.o. informs its customers through contracts concluded according to the Business Terms and Conditions of Gas Supply and in the Business Terms and Conditions of Electricity Supply in an incomplete and inaccurate extent and does not provided information about whether personal data processing for the purposes of concluding contracts is mandatory or voluntary and does not inform customers about the consequences

of refusing to provide personal data, it breached Article 11(2) of Act No. 101/2000 Coll.

The inspections taking place at ČEZ Prodej, s.r.o. and at O2 Czech Republic a.s. are still underway.

The common denominator of all shortcomings ascertained with respect to observance of Act No. 101/2000 Coll. is the lack of clarity and the substantial ambiguity in text informing data subjects about their rights and obligations when concluding contracts and about granting (or refusing to grant) consent with the processing of their personal data for purposes required by law and requiring clients to consent in cases when a company has the right to process personal data without consent under the law.

## E. SEPARATE CONTRIBUTIONS

### **Inspection of [www.scio.cz](http://www.scio.cz), s.r.o.**

In mid 2014, an inspection of [www.scio.cz](http://www.scio.cz), s.r.o. (the "Inspected Entity") was commenced based on a complaint. The complainant stated that in February 2014 she filed an application to a university (the "University"). In March, the complainant received an e-mail offer for external testing sent by the Inspected Entity, stating that she had been contacted based on a database of applicants provided to the Inspected Entity without her consent by the University to which she sent her application.

The Office's inspection commenced an inspection at the company regarding observance of the obligations of a data controller/processor under Chapter II of Act No. 101/2000 Coll. and Act No. 480/2004 Coll., on certain information society services, in connection with the processing of the personal data of university applicants.

Based on a Contract for Works concluded pursuant to Section 536 et seq. of Act No. 513/1991 Coll., the Commercial Code, (the "Contract") with the University, the Inspected Entity, as the contractor, undertook to develop a structured database of results of the National Comparative Examinations - General Educational Expectations (the "Examination") of those applicants applying for Bachelor's studies in fields taking into account the Examinations and to develop a database of the Examination results for the subsequent Master's studies.

According to Contract, the University undertook to provide the contractor with a list of applicants that are registered as applicants who filed an e-application for Bachelor's studies and subsequent Master's studies for the 2014/2015 academic year and paid the application fee.

Pursuant to Section 50 of Act No. 111/1998 Coll., on universities, the entrance procedure commences at the moment of delivery of the application for studies to the university or department thereof that runs the respective study programme. The applicant always states their name or names, surname, personal identification number, if one has been allocated, and permanent address in the Czech Republic or place of residence outside the Czech Republic.

Although Act No. 111/1998 Coll. anticipates the processing of the personal data of applicants for studies, it specifies that only the entities listed in Section 2 thereof can do so. It is thus not possible by definition to infer that the processing of the personal data of applicants for studies can be carried out by any private or public body unless such power (authority) stems from some other special law, processing agreements or consent granted by data subjects. It is clear from the documents provided by the Inspected Entity and the complainant's application for studies

that neither the data controller (the University) nor the data processor (the Inspected Entity) had permission from the complainant to have her personal data handed over to the Inspected Entity for processing.

According to Article 7 of Act No. 101/2000 Coll., the obligation set out in Article 5 also applies to the data processor. From the wording of Article 7, however, it cannot be inferred that all of the obligations apply to the processor, as the observance of all obligations set out in Article 5 of Act No. 101/2000 Coll., cannot be demanded of the processor. It ensues from the Contract, which corresponds to the requirements of Article 6 of Act No. 101/2000 Coll., i.e., to a processing agreement, that for the case at hand (the handover of personal data for the purpose of developing a structured database), it is the University, as the data controller, who bears primary responsibility for demonstrating the legal grounds for processing the personal data of applicants for studies, i.e., for handing over personal data to third parties.

The inspection thus did not ascertain any breach of the provisions of Article 5(2) of Act No. 101/2000 Coll. by the Inspected Entity.

Nevertheless, Section 7 of Act No. 480/2004 Coll. provides protection against the unauthorised dissemination of commercial communication. According to Section 10(1)(a) of Act No. 480/2004 Coll., supervision over observance of this law for disseminating commercial communication is entrusted to the Office for Personal Data Protection. The term dissemination of commercial communication pertains to all forms of communication intended for the direct or indirect promotion of goods or services by a specific entity, provided this entity is an economic entity, i.e., an entity carrying on business activities. According to Section 7(2) of Act No. 4780/2004 Coll., the details of electronic contract information can be used for the purpose of disseminating commercial communication if the users granted their consent.

Effective 1 August 2006, Section 7 of Act No. 480/2004 Coll., was amended by Act No. 214/2006. This amended introduced the opt-out principle, provided this commercial communication is sent by electronic means to the customer's address or to entities in already existing business relationships. Thus, natural or legal persons who received electronic contract information from a customer in connection with the sale of goods or services can use this electronic contract for disseminating commercial communication regarding their own similar products or services without needing to obtain prior consent with using the electronic contact information for the purpose of disseminating commercial communication from their customers.

The inspection findings show that the Controlled Entity collected data for sending commercial communication from various sources. The databases taken from the faculties of various universities containing personal data were the source of contact information for sending the e-mail communication that was the subject of the inspection.

On 1 January 2012, Act No. 468/2011 Coll. took effect. This law amended Act No. 480/2004; specifically, the definition of commercial communication in accordance with Section 2(f) was amended to expand the definition of commercial communication to include advertising and suggestions to visit websites intended for the direct or indirect promotion of goods or services or the image of a person that is a business or runs a licenced business. In order for a message to be considered commercial communication, it is necessary to assess the actual content in its entire context. If the message contains information about a certain offered services, i.e., the possibility to be accepted without undergoing entrance exams based on the results of the National Comparative Examinations which replace or supplement the entrance exams at dozens

of universities in the Czech and Slovakia for a fee, such message is deemed direct or indirect promotion of goods or services offered by the Inspected Entity and in accordance with Article 2(f) of Act No. 480/2001 is thus commercial communication. It stems from the e-mail message/commercial communication sent to the complainant and the Inspected Entity's declaration that the footer of the e-mail message describes how to request that information e-mails be stopped. It is thus clear that although the Inspected Entity consider the e-mail messages to be "information e-mails", they are also commercial communications serving to directly or indirectly promote the Inspected Entity's goods and services. The Inspected Entity confirmed in writing that it in fact did send such message and that the distribution thereof is arranged by a different company.

The Inspected Entity did not have the prior consent to disseminate the commercial communication with the subject "possibility to be accepted at university without entrance exams" from users in accordance with Section 7(2) of Act No. 482/2004 Coll. The inspection thus ascertained a breach of Section 7(2) of Act No. 480/2004 Coll.

### **Lists of association members**

The Office's inspector, based on an instigation, conducted an inspection, the subject of which was observance of the obligations laid down in Act No. 101/2000 Coll., with a focus on the protection of the personal data of members of the Firefighters Association of Bohemia, Moravia and Silesia (Sdružení hasičů Čech, Moravy a Slezska -- "SH ČMS"). The instigation made reference to publication of the list of SH ČMS members on [www.ulozto.cz](http://www.ulozto.cz). The inspection of SH ČMS, as the controller of the personal data of its members, was aimed at observation of Article 13 of Act No. 101/2000 Coll., i.e., technical and organisational safeguarding of personal data.

According to the instigation, a database file of SH ČMS containing approx. 359 000 pieces of personal data of association members was available on the internet portal [www.ulozto.cz](http://www.ulozto.cz) for downloading. The member databased was stored on <http://ulozto.cz/xgbGFok/seznam-clenu-xlsx>. The file was uploaded to [www.ulozto.cz](http://www.ulozto.cz) on 21 March 2013 and was removed immediately (on the same day) upon the media calling attention to this fact. The file, which was in Excel format and of a size of 72.99 MB, contained the personal data of 329 690 members of SH ČMS, specifically: the district branch of the association to which the member belonged, name, surname, date of birth, age, sex, name of club, registration number, personal identification number, contributions to headquarters, contributions to the club and position (trainer, referee, registered athlete, functionary, member of the technical/organisational staff or other position).

According to SH ČMS representatives, the data file was stored on [www.ulozto.cz](http://www.ulozto.cz) by an authorised person so that the administrator could download it as the size of the file of approx. 70 MB made it impossible to be sent by e-mail. The personal data was provided to the authorised person (the "processor") so that he could complete or, more precisely, amend them so that the file (personal data) would correspond to the requirements of the Ministry of Education, Youth and Sports ("MoEYS") as part of SH ČMS's application for a government grant for sport, i.e., the database file created by the processor needed to be checked before being sent to the MoEYS and due to the size of the file and time frame for handing over the data, the processor and the SH ČMS office representative chose to send this file via the web portal [www.ulozto.cz](http://www.ulozto.cz).

SH ČMS assessed the data in the file as harmless as in SH ČMS's opinion, the information was not of the extent that would allow the members to be attacked via telephone, e-mail or place of residence. The data in question was name and date of birth. SH ČMS also stated that it is not even a rule that a person is a member of the association where they have their place of residence. And, in the case of SH ČMS, the name of the town is not the town where the member lives, but of the organisation of which the person is a member. The representatives of SH ČMS further stated that based on their own experience, they assessed the wording of the Personal Data Protection Act to be as follows: personal data should not be published if there is the possibility of a person being addressed directly and that the data was not disclosed to a third party and should have been on the server for just a few hours before the file was downloaded and deleted. The SH ČMS representatives further stated that: "This unfortunate incident was caused by the fact that the programmer who usually placed data on the VPN (virtual private network), which in this case serves to transfer data between the processor and the person authorised to administer the programme from the point of view of the needs of SH ČMS, was not available. We needed to share the entire data file in order to check it and as it was so large, we decided to use the Uložto server."

The SH ČMS representative further stated that the "file containing the records of members was drawn up by the processor on his own computer at his place of work and place of residence. After completing it, he sent it as an unencrypted and not coded document through the ulozot.cz web portal. He sent it in this way because he did not realise that the document could be misused. Immediately after learning that reporters were interested in the case, access to the file was blocked and removed from www.ulozto.cz."

The file was created from the primary database of SH ČMS members, which is stored on a server in the USA through cloud services.

The membership records programme is also necessary for obtaining funding from grants of the ministries and regions, as the ministries expressly require extracts from membership records in electronic form with applications.

The inspector stated in the inspection protocol that the membership records are based on applications that are at the same time used as the members' personal cards. The information collected and then processed in SH ČMS's records is information that is used to clearly identify a specific member of the association. The information collected and processed in connection with maintaining the SH ČMS membership records is personal data under Article 4(a) of Act No. 101/2000 Coll., as this information pertains to a specific data subject that is directly determinable based on the collected information.

SH ČMS collects information about its member from membership applications and stores it in its files and then supplements the files with information about their activities once they become members. Furthermore, it systematically stores the information in hard copy form and through the "membership records" programme collects it, stores it on carriers, searches for it and uses it for its activities or the activities of its various branches, i.e., it processes the information in accordance with Article 4(e) of Act No. 101/2000 Coll. At the same time, SH ČMS decided not only about the purpose of the processing, but through the articles of association, organisational rules and agreements about the means of processing the personal data of its members; as such, is a personal data controller according to Article 4(j) of Act No. 101/2000 Coll. and is responsible for such processing.



SH ČMS concluded with a natural person doing business pursuant to the Trade Licencing Act an agreement on the creation of an electronic membership database and its subsequent processing. In terms of Act No. 101/2000 Coll., this natural person was a personal data processor because, as an independent entity based on the authority of SH ČMS, processed the personal data of association members. SH ČMS thus decided to disclose and subsequently have the personal data of association members processed by the processor for the purpose of delivery to a membership web application and operation of such application. SH ČMS, as the personal data controller, concluded an agreement with the processor in writing. The subject of the agreement is the transfer of the personal data of association members from the current membership records to a new, centralised SH ČMS membership database. The association, as the personal data controller, concluded a written agreement with the processor concerning its scope, purpose and duration. The agreement contained no guarantee by the processor of the technical and organisational safeguards to protect the personal data. The agreement contains the processor's undertaking to execute the works at own costs and risk. When determining the way the works should be carried out, he shall not be bound by the client's instructions, and when having the works executed by a different person, he shall take responsibility for the execution as if he executed the works himself. Furthermore, he shall protect the data files and the client's data from damage, destruction, misuse and theft at his own cost and risk. An agreement concluded in this way cannot be deemed fulfilment of a personal data controller's obligations under Article 6 of Act No. 101/2000 Coll. even if the content of the agreement is the migration of data from the various existing systems to a newly created database file, as the purpose of Section 6 is the imposition of the obligation on the personal data controller to verify and by agreement approve guarantees that the processor will provide technical and organisational safeguards of personal data when this data is in his possession. Furthermore, SH ČMS, being the personal data controller, cannot relieve itself of responsibility in this way, and without any knowledge and guarantees allow the processor to disclose the personal data of its members to a third party, as in this way the administrator curtails the data subjects' rights to have their personal data under control, such right being set out not only in Article 11(1) of Act No. 101/2000 Coll., according to which the personal data controller is also obliged to provide information about who will be processing the personal data and in what way, but also in Article 12 of Act No. 101/2000 Coll., i.e., the data subject's right to information.

By passing the processing of the personal data of its members on to the processor without having him commit to protecting the personal data and without contractually reserving the right to control the data, SH ČMS contented itself with general information that the entire membership database is stored in a cloud on a server located in the USA without contractual guarantees from the cloud operator. SH ČMS then failed to take any measures against such entirely unsecured personal data processing. Under Article 13(2) of Act No. 101/2000 Coll., a personal data controller is obliged to process and document adopted and implemented technical and organisational measures to safeguard personal data in compliance with the Act No. 101/2000 Coll. and other legal regulations. The basic activities of SH ČMS are governed by the association's Articles of Association and Organisational Rules. Both of these legal documents only govern the basic obligations of various branches of SH ČMS concerning operations and the safeguarding of information.

SH ČMS did not present any documents, internal regulations or adopted measures that would show how the responsible person entrusted with management of the data was incorporated organisationally in SH ČMS and to whom such person is responsible. Furthermore, it failed to document any that it has any measures in place for checking observance of the rules for transmitting and sharing data between branches, checking access to data, or checking the security of IT technology, especially checking that the contractual personal data processor is fulfilling his obligations. SH ČMS did not adopt any measures for handing over and storing the personal data of members in a cloud repository on a server in the USA, nor did it adopt any measures with respect its data processor.

It is clear from the above that SH ČMS failed to fulfil its obligations as a personal data controller under Article 13(2) of Act No. 101/2000 Coll., i.e., to process and document adopted technical and organisational measures to ensure that personal data is protected.

A consequence of the fact that SH ČMS did not fulfil its obligation under Article 6 of Act No. 101/2000 Coll. to incorporate in the personal data processing agreement guarantees on the part of the processor to protect personal data through technical and organisational measures and the fact that SH ČMS did not fulfil its obligation to adopt and document technical and organisational measures, and the fact that SH ČMS did not undertake any controls concerning personal data protection, the association's complete membership database was made available in unsecured form on the website [www.ulozto.cz](http://www.ulozto.cz).

By making the data of 359 690 SH ČMS members available on [www.ulozto.cz](http://www.ulozto.cz) in an unsecured form for a period of less than a day, it breached its obligations as a personal data controller pursuant to Article 13(1) of Act No. 101/2000 Coll., i.e., to adopt such measures that would prevent unauthorised or chance access to personal data. By failing as a data controller or through its processor to arrange for electronic records (logging) that would allow it to determine and verify when, by whom and for what reasons the personal data was recorded or otherwise processed in the membership database, SH ČMS breached its obligations under Article 13(4)(c) of Act No. 101/2000 Coll.

SH ČMS was then, as part of administrative proceedings, imposed a fine of CZK 80,000 for violating Act No. 101/2000 Coll.

Based on the above inspection, an inspection of MoEYS was commenced as part of the Office's control plan for 2014, the subject of which was the observance of a personal data processor's obligations set out in Chapter II of Act No. 101/2000 Coll., in connection with the processing of personal data in documents pertaining to subsidies provided by the Ministry of Education, Youth, and Sports in the form of State Support for Sport for 2013 and 2014. The inspection is still underway.



# OTHER SUPERVISORY ACTIVITIES

- COMPLAINTS HANDLING AND CONSULTATIONS

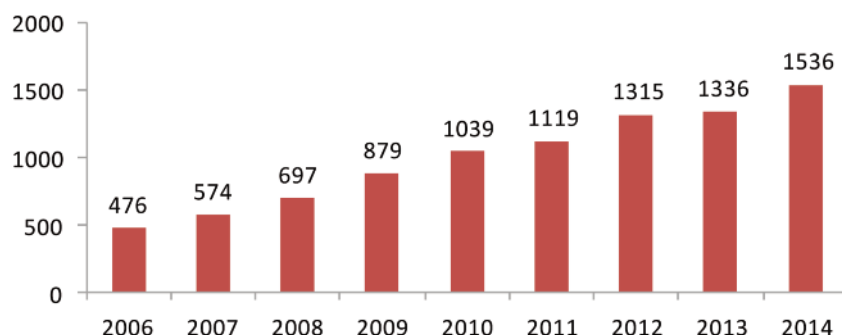
Based on what the Office has learned by handling complaints and providing consultations, such activity being in the remit of the Public Relations Department (Odbor pro styk s veřejností – “VER”), it is possible with the nearing 15th anniversary of the force of Act No. 101/2000 Coll. to confirm greater awareness of personal data processing and the Office’s activities among the public and among personal data controllers and other stakeholders. This is apparent not only by the ever increasing number of accepted filings (complaints/instigations and questions) that the Public Relations Department dealt with in 2014 compared to previous years but also by the character and complexity of such filings and consultation topics.

Standing behind the growth in the number of filings this year is chiefly the increase in the number of complaints compared to last year, when the number of accepted complaints stagnated, as showed by the graph below.

Total number of queries and complaints/instigation processed by VER



## Number of instigation/complaints received by VER



The greater number of received complaints was also reflected in the number of cases that were forward by the Public Relations Department for further action, i.e., for inspection (237) or for administrative proceedings (49). Twenty-one filings were forwarded to the appropriate administrative bodies for further processing in compliance with Section 12 of Act No. 500/2004 Coll., the Code of Administrative Procedure.

A current topic of the complaint and consultation agenda is the “right to be forgotten”, which was an important personal data protection topic on the internet in 2014 as a result of a decision of the Court of Justice of the European Union in the matter of Google v. Costeja. In this decision, the Court of Justice of the European Union expressed its opinion that people have the right to have outdated or irrelevant results of searches related to them removed, i.e., the decision has to be applied to all search engines, not only to the search engine operated by Google Inc. The decision of the Court of Justice of the European Union, however, does not make it possible to eliminate all results of searches concerning a specific person as is erroneously interpreted to the public.

In other aspects, the complaints agenda was similar to that of previous years, i.e., the most commonly received complaints traditionally revolved around the operation of camera surveillance systems (at the workplace, in public space) and debtor registries, especially in the SOLUS registry and the Central Registry of Debtors of the Czech Republic. Complaints regarding offers for sale of databases of e-mail contact information and other personal data or the issue of personal data processing in labour law relationships and health care are also worthy of mention. Complaints regarding personal data processing by local governments, especially municipalities, form a substantial part of the complaints agenda.

As part of the assessment of the received complaints, suspicion of violation of Act No. 101/2000 Coll., regarding the lack of legal grounds to process personal data or the failure to observe other conditions for personal data processing stipulated by Act No. 101/2000 Coll., was the most common complaint. This concerned for example the collection of superfluous personal data, processing of personal data for some other purpose than for which it was collected and, last but not least, the insufficient safeguarding of personal data or, more precisely, leaks thereof.

In the case of the Office's consultation activities, carried out mainly in the form written correspondence but also by telephone and in person at the Office's premises, the most frequent consultations pertained to the conditions for using camera surveillance systems, where it is necessary to differentiate between camera surveillance systems falling under Act No. 101/2000 Coll. and cameras installed for personal use in family homes, provided they do not record the public realm, and particularly the use of police camera systems, which is regulated by law. Provisions are also made for the difference of cameras used in cars for monitoring the premises while the vehicle is in operation.

Questions about the statutory conditions for obtaining copies of personal documents, especially personal identity cards in connection with concluding agreements on the provision of electronic communications or banking services, are also frequent. Even questions about the justification of requests for personal identification numbers in various life situations were also common.

The Office also encountered questions about the statutory conditions for publishing the personal data of citizens on the websites of municipalities, where publication takes place based on a special law, i.e., without the citizens' consent, and the publication of audio-visual recordings from meetings of municipal councils with redacted data regarding the private lives of citizens.

The difference between banking and non-banking registries of debtors is another consultation topic.

It is often necessary to explain to enquirers the difference in the way these registries are kept in terms of the conditions (legal grounds) for processing personal data according to Act No. 101/2000 Coll. Banking registries process personal data according to Act No. 21/1992 Coll., on banks, and thus do so without the consent of the bank's clients in compliance with Article 5(2)(a) of Act No. 101/2000 Coll.; non-banking registries process personal data based on the consent of the data subject unless the processing is required by law. Other possibilities for exercising certain rights available to data subjects, especially when it comes to the period that personal data can be stored, ensue from this difference.

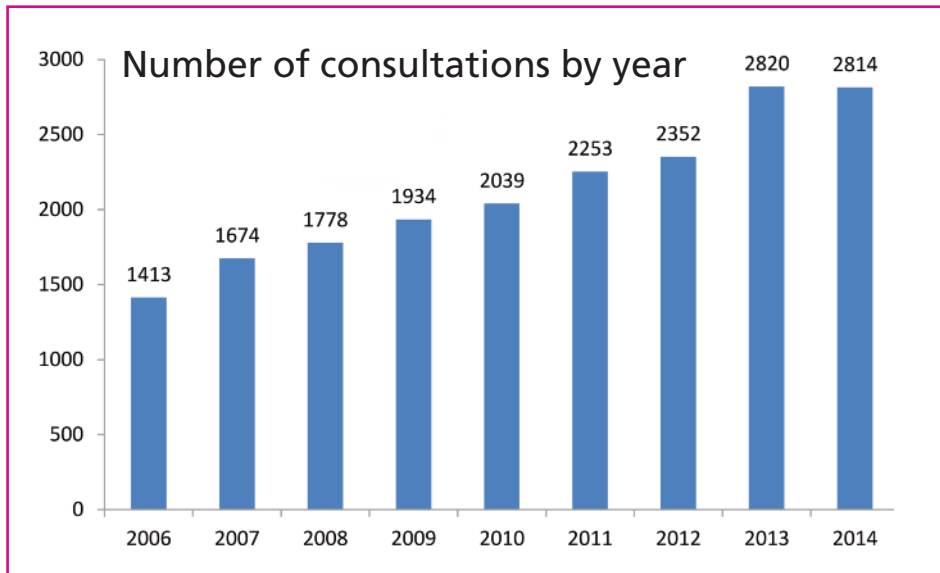
As regards information systems of public administration, a frequent subject of questions is the public nature of the insolvency register and the possibility to limit the information being made public on such registers, especially as regards the data of creditors or employees. The questions also pertain to the possibility of making use of personal data from other publicly accessible registers, such as the Trade Licence Register and Cadastral Register.

Municipalities often have questions about the disclosure of their representatives' or employees' personal data based on requests under the Act on Free Access to Information, especially data about salaries and bonuses in light of the newest ruling of the Supreme Administrative Court (No. 8 As 55/2012) in this matter.

There were even questions concerning the use or misuse of personal data (especially in the environment of the internet) outside the confines of Act No. 101/2000 Coll., where it is usually stated that the handling of personal data does not always constitute personal data processing as this term is defined in Act No. 101/2000 Coll., and a civil law approach or the approach outlined in Section 5 of Act No. 480/2004 Coll. is recommended.

In 2014, the Office obtained a number of questions and complaints regarding the use of camera systems for protecting buildings belonging to embassies in the Czech Republic. For this

reason, a brief methodology describing the basic rules for such processing of personal data was prepared in cooperation with the Ministry of Foreign Affairs. This methodology was distributed in November 2014 in the form of a circular note to all foreign embassies in the Czech Republic.



## ● SOME FINDINGS OBTAINED IN ADMINISTRATIVE PROCEEDINGS

Administrative proceedings at the Office are conducted primarily (but not exclusively) by the Administrative Operations Department.

Essentially two types of proceedings are conducted through the Administrative Operations Department: proceedings on administrative offences and proceedings in cases where concerns are raised that Act No. 101/2000 Coll. could have breached when personal data was processed (see Article 17 of this Act).

Both types of proceedings are conducted by the Office by virtue of its position, i.e., *ex officio*.

In 2014, based on an amendment of Act No. 101/2000 Coll., the Office gained the possibility not to impose fines in cases where the unlawful state was remedied immediately after the breach of obligations was discovered (see Article 40a thereof).

### 1. Proceedings under Article 17 of Act No. 101/2000 Coll.

Regarding these proceedings, which are tied to the data controller's notification duty under Section 16 of Act No. 101/2000 Coll., it needs to be emphasised that these proceedings are not penal proceedings. Their objective is, simply said, to regulate the notified parameters of personal data processing into a form that corresponds to statutory requirements. Thus the focal point of such proceedings is found in oral proceedings with the party to the proceedings (i.e., the person who is the data controller in relation to the notified processing) where the party to the proceedings provides the Office with all details about the intended processing and the Office staff, in connection with this information, clarifies the conditions under which the processing can be carried out. Usually a change in the notified processing follows, and the party to the proceedings implements such change based on information ensuing from the oral proceedings. At the same time it needs to be stated that such proceedings almost 100% of the time pertain to notified personal data processing via camera surveillance systems. It can be stated that (as ensues from the relevant statistics) in the last three years, more than 95% of such proceedings have been adjourned with the conclusion that the notified processing will not lead to the data controller breaching his obligations under Act No. 101/2000 Coll. and that the processing is, based on such decision, entered in the register maintained by the Office. In the remaining cases, the Office does not allow the processing (in 2014 this concerned, for example, a camera surveillance system located in a hostel, inside buses and in a residential building).

The basic problem that the Office contends with during these proceedings is the fact that although the data controller is obliged to report processing before the intended processing takes place, the camera surveillance systems through which the personal data should be processed are often already in operation or, if not in operation, already installed in the respective premises. Changes in the way the various cameras are set up, something that often takes place during proceedings, may mean additional financial expenditure tied to the fact that the data controller did not begin to deal with the conditions for operating the whole system unit an inopportune phase (that is not before the installation of the system itself as the data controller should have). Although the technology is of a kind that allows for numerous additional

measures to take place (such as the use of a grid), there is no doubt that it is more advantageous for the data controller to address the intended processing, which includes the specific set up of the various cameras, as soon as possible.

## 2. Option not to impose a fine

Act No. 64/2014, which amends certain acts in relation to the adoption of the supervisory rules, introduced an entirely new Article 40a to Act No. 101/2000 Coll., effective 1 May 2014. According to this section, if the unlawful state is remedied in accordance with the imposed measures or immediately after the breach of obligations was discovered, the Office can opt not to impose a penalty.

This is a provision that should be lauded. What needs to be noted here is that the penalties imposed under Act No. 101/2000 Coll. for a breach of the statutory obligations have a very high upper threshold (i.e. CZK 100 000 for a breach of confidentiality obligations and CZK 1 000 000 - CZK 10 000 000 for breach of the data controller's or processor's obligations). Fortunately, the law does not and has never stipulated the bottom threshold because with the upper threshold set so high, the bottom threshold would also have to be set relatively high, and so would be financially ruinous for many data controllers, who are often individuals/non-entrepreneurs.

Until the end of April 2014, however, there was no way not to impose a penalty if a breach of obligations under the law was discovered and such breach was at the same time an administrative offence. Such approach would not be possible even in the case of relatively banal actions, where the responsible persons remedied their error immediately after they were informed about it. Article 40a of Act No. 101/2000 is changing this situation.

This of course does not mean that the Office, when applying the provision, would be able to act entirely at will, as it is obliged, inter alia, to observe the basic principles that apply to administrative bodies in Section 2 et seq. of Act No. 500/2004 Coll., the Code of Administrative Procedure, especially the principle of protection of legitimate expectations. In order for the Office to observe these obligations, it modified the application of Article 40a of Act No. 101/2000 Coll. by Internal Directive No. 5/2014, which states the conditions for waiving a fine. According to this directive, it is possible to waive a fine if the unlawful state is remedied in compliance with imposed measures or immediately after the breach of obligations is discovered and the following conditions are met at the same time:

- the conduct does not relate to a breach of obligations in connection with processing sensitive data
- the conduct does not infringe on the rights of a greater number of data subjects
- the conduct does not represent a substantial infringement of the rights of data subjects
- a combination of the circumstances set out in Article 46 of Act No. 101/2000 Coll. would sustain the imposition of a penalty of up to CZK 5000.

The fact that the provision in question can be applied by the Office in practice is documented by the statistics of the Administration Operations Department, which has waived fines in 17 cases based on the mentioned provisions. For example, there was a breach of Article 12 of Act No. 101/2000 Coll., i.e., the obligation of the personal data controller to hand over information about personal data processing to a data subject without undue delay at the request of the data subject; a breach of Article 5(1)(f) of Act No. 101/2000, i.e., the obligation of the personal data controller to process personal data only in compliance with the purpose for which

such data was collected, in this case publishing data on the website of a municipality (there were a number of such cases).

In conclusion, it can be stated that this legislative change is highly appropriate – at least from the point of view of the Office’s practice – as it moves the Office’s role of imposing sanctions to second place and allows the Office to focus instead on fixing the unlawful state, which should be the Office’s primary objective (of course, only if it is possible, as there are without a doubt numerous cases when it is not possible to remedy the unlawful conduct of the accountable entities).

## ● FINDINGS FROM JUDICIAL REVIEWS

Certain decisions of the Office are subject to judicial review. As regards the specific findings from judicial practice for 2014, it is possible to call attention to a number of important decisions, discussed below, pertaining in particular to camera surveillance systems, disclosure of operational and localisation data, implementation of remedial measures, personal data processing in the framework of television broadcastings and obligations in connection with the safeguarding of personal data.

1. Supervision undertaken with the help of video cameras at the workplace is possible only in the event that the stipulated purpose cannot be fulfilled through less invasive means; the stipulation of the deadlines for the processing of recordings need to be adjusted to this purpose. Fulfilment of the information obligation under Article 11 of Act No. 101/2000 Coll. is dependent on the group of persons being monitored. In case of doubt, the data controller should request consultation pursuant to Article 29(1) of Act No. 101/2000 Coll.

In Decision No. 8A 182/2010-69 dated 2 September 2014, the Municipal Court in Prague expressed in particular the opinion that employees have the right to a certain degree of privacy even at work, even though due to the nature of the employment relationship it is less than, e.g., in one's own home, as personal and private life cannot be entirely separated; a person carries a bit of their private life with themselves at all times and a camera system monitoring employees is a significant infringement of privacy in that they are monitored every day continuously during working hours or for a large part thereof.

The Municipal Court in Prague in its Decision No. 8A 182/2010-69 dated 2 September 2014 added that concealed monitoring is in this regard a greater infringement of privacy than informed monitoring; both types of monitoring, however, infringe on privacy. In the case at hand, the resolution of the cameras was so high that it was possible to identify individual persons (employees), including minor details, and because the camera took recordings every 5–10 seconds, their activities could be monitored in detail for most of their working hours; a significant infringement of privacy thus did in fact take place. As regards the declared purpose – i.e., checking opening hours, monitoring working hours and distributing the work load – the chosen purpose was apt as it made it possible to ascertain when and which employee was located on the sales premises; however, it is clear that the employer could have chosen less invasive means, e.g. chip cards or cameras monitoring only the entrance to the shop, and that it was not necessary to monitor employees directly at the sales counter; it was also possible to monitor employee performance even according to the achieved results.

The employer then only listed the protection of property, specifically games consoles located along the perimeter of the shop, and especially protection against unauthorised provision of discounts by employees as the purpose of the camera system. In this connection, the Municipal Court in Prague stated that the archived images showed that a camera was located in each of



the 20 shops belonging to the employer. With one exception, the cameras were recording only a part of the shop, specifically a section of a few metres, but in each case it was directed at the sales counter and cash desk. The camera system could thus not have served as effective protection against theft of the games consoles, as it did not monitor the parts of the shop where they were located. In the monitored space of the sales counter, any theft would have been in the presence of the shop assistant. The Municipal Court in Prague added that with regard to the size of these devices, a camera monitoring the entrance to the shop would have been a sufficient form of protection.

At the same time, it was reiterated that the need to monitor the sales counter was originally justified by the fact that employees often provided discounts to non-existing customers, and in this way it was possible to retrospectively verify whether a real customer was present at the counter at the time of sale. In this regard, the Municipal Court in Prague of course stated that such misuse could have been prevented by modifying the discount programme; even if such modification would be too complex, the employer could have positioned the cameras to record the space in front of the sales counter and not the space behind it where employees spend most of their time; in this way the employer could have verified the presence of a customer by the counter and at the same time protected the privacy of the staff. The Municipal Court in Prague also stated in this case that the employer, in order to ensure the privacy of his employees, could have used less invasive means. For this reason, it processed personal data at variance with Section 5(2) of Act No. 101/2000 Coll.

The Municipal Court in Prague also dealt with the issue of the period that personal data is retained for. Pursuant to Section 5(1)(e) of Act No. 10/2000 Coll., a data controller is obliged to retain personal data only for the period that is required to process it. The employer, i.e., the personal data controller, set this period at one year, during which it stored all images recorded. It justified this practice only by stating that it was suspicious that staff members were providing unjustified discounts and in order to check this, it was necessary to compare the cashier data (the time that discount was provided) with the camera system that would show whether a real customer was present when the discount was given. It is clear from the above that the personal data controller recorded all times when the sales were provided; therefore, there was nothing preventing him, when transferring images from the computer to CD or DVD, which occurred on a monthly basis, from retaining only images recorded at the time when, according to the data from the cash register, the staff provided a discount. As in the vast majority of processed images it was sufficient to retain them for no more than a number of weeks, it had to be clear to the data controller that the period of one year exceeds the period necessary. In this connection, the personal data controller's reference to the ambiguity of Article 5(1)(e) of Act No. 101/2000 Coll. does not pass muster.

As regards the notification duty under Article 11(1) and (5) of Act No. 101/2000 Coll., it is necessary to take into account the fact that in relation to random passers by (e.g. customers), it is virtually unrealistic to fulfil this obligation and it is sufficient to provide basic information that a camera surveillance system is installed in the respective location with a notice stating who the system administrator is or where it is possible to obtain information about the personal data processing underway. It is especially important, however, that it be stated who is the operator of the camera surveillance system. Conversely, if the group of persons who are to be monitored is known in advance (typically employees), full information has to be provided.

If the personal data provider had doubts about how reasonable the imposed measures were, he could have requested a consultation with the Office pursuant to Article 29(1) of Act No. 101/2000 Coll., but he had not done so.

## 2. Operational and location data recorded and stored pursuant to Section 97(3) of Act No. 127/2005 Coll., on electronic communications, may not be made accessible with a reference to Article 40(1)(a) of Act No. 121/2000 Coll., the Copyright Act

The Municipal Court on Prague, by way of Decision No. 31C 1/204-88 of 21 August 2014, dismissed a petition which requested disclosure of operational and localisational data recorded and stored pursuant to Section 97(3) of Act No. 127/2005 Coll. simply by referencing Article 40(1)(a) of Act No. 121/2000 Coll. mainly for the reason that the data in question had already been destroyed. Nevertheless, the court essentially recognised the argument that that handling operational and localisational data is strictly regulated by Act No. 127/2005 Coll., with this regulation being *lex specialis* in relation to Act No. 121/2000 Coll. The provider of internet connection services may disclose the data in question only based on this special regulation and, what is more, only under circumstances foreseen by this special regulation. This obligation does not pertain in any way to persons exercising copyrights or other similar rights, whereas it is not possible to apply the general provisions of Article 40(1)(c) of Act No. 121/2000. It also has to be kept in mind that a single IP address can be allocated to a number of users at one specific moment. It is also important to reiterate that the Court of Justice of the European Union has concluded that European legislation only does not prohibit (i.e., it does not order) the adoption of national legislation according to which it would be possible to satisfy what was requested in the petition. In the Czech Republic, however, such specific regulation has still not been adopted.

## 3. If the inspected entity intends to call attention to the fact that it is being imposed obligations that no longer correspond to the current state of affairs, it is important that it do so in its objections to the inspection protocol

The Supreme Administrative Court stated in its Decision No. 3 As 124/2013-34 of 30 July 2014 that abandoning the contested practice (in this case operation of the respective camera surveillance system) by the personal data controller could in reality only have happened once it was clear what was being demanded of him, i.e., after the respective remedial measures were first formulated in the inspection protocol or only after a decision was made on objections filed against the inspection protocol, where the majority of the imposed measures were confirmed by a decision issued by the Office President. In such situation, however, the data controller could do little else but remedy the ascertained situation immediately, although the remedy, which method of implementation was chosen by the data controller, went above and beyond what was required in the respective measures (the measures did not require abandoning the practice of making recordings and processing personal data completely, but only specifying the operation of the camera surveillance system and duly and fully informing people about its operation).

Even after taking the above into account, the Supreme Administrative court stated that it could do little else but reiterate that if the data controller did in fact mean what he claimed, i.e., the inspection protocol imposed obligations on him for such fictitious state that no longer corresponded to the actual state, then it is entirely inconceivable and illogical that the data controller did not file objections to the inspection protocol when doing so would be clearly in his primary interest. Any objections filed at a later time can only be seen as observing some ulterior motive. This argument is further supported by the fact that despite the data controller's objection that its timely abandonment of the practice of making recordings and processing personal data made it no longer necessary to impose any measures, he contested the imposed measures even in terms of substance.

#### 4. Preparation of a television report aimed at disclosing personal data through broadcasting is personal data processing in accordance with Act No. 101/2000 Coll.

The Supreme Administrative Court stated in its Decision No. 6 As 144/2013-34 of 20 August 2014 that it has no doubt that the broadcasting of a television report in which a person suffering from communicable disease was identified by name and surname is personal data processing in accordance with Act No. 101/2000 Coll. The essence of television broadcasting is activities that are, in connection with preparation as well as with the broadcasting itself, carried out in a targeted, organised and regular manner. The procurement and publication of the respective information included a number of steps, from reviewing police websites through investigative activities to obtain additional information the behaviour of the data subject from third parties, deliberation about the characteristics of the way the disease was transferred or other investigation with the aim of identifying it exactly, to the technical processing of the report, including it in the news report and broadcasting it. In this process, which ended with the disclosure of the data subject's diagnosis in a national broadcast during prime time, there is no room for inadvertence. The fact that the information was broadcast only once does not mean that there was no systematic work attributable to the data controller. The respective deed has to be looked upon comprehensively, as the activities preceding the disclosure through broadcasting fundamentally and inseparably relate to the final act. The inadvertent disclosure of the person's state of health would not have such a background.

#### 5. Exerting all efforts that could be demanded in accordance with Article 46 of Act No. 101/2000 Coll. does not mean any efforts undertaken by the data controller, but has to mean maximum possible efforts that the controller is objectively able to exert in relation to each specifically assessed case. The fact that a concluded contract for works contained a detailed description of the procedure from taking over specific waste from the controller by another responsible person is not sufficient to relieve the controller of responsibility

In its Decision No. 11A 107/2013-28 of May, the Municipal Court in Prague stated that the rules for protecting personal data essentially apply in all circumstances. It is irrelevant whether

the personal data is processed as an electronic file or as a set of paper documents. Exerting all possible efforts in accordance with Article 46 of Act No. 101/2000 Coll. does not mean any efforts undertaken by the data controller but maximum possible efforts that the data controller is able to exert in relation to each specifically assessed case. If the parties concluded a contract for works regarding the immediate disposal of items containing sensitive personal data with the mentioned items then being found in a public dump, which is surely not a place usually chosen to store documents containing personal data, then the situation is not one of exerting maximum effort to prevent unauthorised access to this data. The instructions were incorporated into the text of the contract but it was not demonstrably shown that they were executed sufficiently to actually prevent leaks of personal data, which means that the data controller did not expend all efforts that could be required, with there surely being other possibilities available to prevent disclosure of personal data. The primary purpose of the obligations under Article 13(1) of Act No. 101/2000 Coll. is not for the personal data controller to formally adopt security regulations but to ensure that no unauthorised access to personal data occurs thereby satisfying the right of the personal data subject to privacy.

With regard to the above interpretation of Article 13(1) of Act No. 101/2000 Coll., the Municipal Court in Prague expressed the opinion that the use of the terms “shall not accept or shall not carry out” does not have any bearing on the character of the data controller’s liability under the mentioned legal provision. Bringing security measures to life so that they fulfil their meaning and purpose cannot be done in any other way than by adoption and implementation, with these two terms concurrently fully covering and describing all possible methods of fulfilling the purpose of security measures. One can do little else but adopt and implement security measures; the wording of Article 45(1)(h) of Act No. 101/2000 Coll. does not provide any room to deny, when proving preventive actions, that the merits of the offence occurred if access to personal data by an unauthorised person was proven without a doubt.

## ● REGISTRATION

The trend of growth in the number of notifications continued in 2014 as well. In this year, the Office received 7686 processing notifications pursuant to Article 16 of Act No. 101/2000 Coll. Compared to the year before, this constitutes a 15% increase. In addition to registration notifications, the Office handled 845 requests regarding amendments to existing registrations. These amendments most often pertained to addresses, changes in the scope of the data to be processed, data subject categories, purpose of processing and place of processing. In addition to assessing the received registration notifications, the Office issues registration cancellation decisions pursuant to Article 17a(2) of Act No. 101/2000 Coll. This year, there were 132 processing cancellations based on the requests of data controllers, most often for the reason that a company was being wound up or merged, entrepreneurial activity was being terminated or personal data processing was being ended. The number of such requests grew by 27%. The Office publishes information about cancelled registrations in its Journal.

Should the notification not contain all of the details necessary for assessment and processing, the data controller is sent a request for additional information. In 2014, the Office commenced 1001 registration proceedings pursuant to Article 16(4) of Act No. 101/2000 Coll. To a great extent, the proceedings concerned processing via camera surveillance systems with recording equipment, processing of sensitive data, processing personal data with clear legal grounds etc. If such proceedings reveal or confirm suspicions of a breach of the law, the Office commences administrative proceedings in accordance Article 17 of Act No. 101/2000 Coll., which can be concluded with a decision to refuse to grant permission to the notified processing. In 2014, such proceedings commenced in the case of 131 submitted processing notifications, which represents an increase of 31% compared to the year before.

The most common notified type of processing, just like in previous years, was personal data processing through camera surveillance systems with recording equipment (about 21% of all filed notifications). A total of 13 711 entities that filed notifications of personal data processing via camera surveillance systems are registered in the personal data processing register (the difference compared to the sum of the various years in the table is due to the fact that a single entity could have filed a notification in a number of different years). In 2014, 2719 entities filed a notification, which is an increase of 12% compared to 2013.

Table 1

Overview of the number of entities that filed personal data processing notifications, regarding camera surveillance systems

Year	Number of entities		
do 2005	32	2011	1505
2006	386	2012	1887
2007	890	2013	2373
2008	1399	2014	2716
2009	1255		
2010	1268	<b>Total</b>	<b>13 711</b>

### **Cameras in automobiles (Dashcams)**

The Office registered an increase in the number of notifications from natural persons (individuals) planning to process personal data through cameras located inside automobiles and monitoring the space in front of the moving automobile for the purpose of using the recordings obtained as evidence in the event of an accident or other insured event. In terms of infringement of the right to protection of privacy and personal data, such processing is considered by the Office to carry little risk (compared to stationary camera surveillance systems, moving ones are not able to provide the operator with a regular overview of the location and behaviour of people in a particular place, nor does it infringe upon the right to habitation). At the same time, it does not expect the recordings from the car camera system to be used for a different purpose (e.g. publication) and need not be the subject of preliminary proceedings conducted by a supervisory body; thus the notification duty under Article 16 of Act No. 104/2000 Coll. does not apply to such processing.

### **Processing via biometric technologies**

As information technology develops, special ways of processing using these new technologies are appearing ever more often. This pertains for example to technologies securing access to special workplaces most often on the basis of fingerprints, the iris or the bloodstream. The last of the three mentioned biometric technologies in particular is beginning to be promoted to an ever greater degree. The Office registered a number of questions and notifications about processing from companies that are planning to introduce these technologies for the purpose of securing access to security zones. The access system contains a biometric scanner that is able to recognise individuals based on an image of the bloodstream in the palm. If the image of the bloodstream is then converted automatically in the system into a biometric template, which is a reduction of the biometric image into a set of numbers that cannot be used to reconstruct the biometric data, the processing is not the processing of sensitive data. A biometric template, i.e., a dimensionless numerical code, is "only" personal data in accordance with the Office's Position No. 31/2009.

This year, the Office also registered a number of notifications regarding the use of dynamic biometric signatures. Specifically, this is data pertaining to its attributes and dynamics, pressure used to draw the signature and the time it takes to draw the signature, all for the purpose of safeguarding and exercising legal claims in case of doubts or a dispute about the authenticity of the signature. The Office issued Position No. 2/2014 on the issue of its use in connection with the application of Act No. 101/2000 Coll. In terms of the fulfilment of the notification duty, the following facts are important: the processing of the dynamic biometric signature is subject to the notification duty, constitutes the processing of sensitive data and, as such, requires express consent from the data subject to its processing.

### **Processing of personal data necessary for using resources from the European Funds**

As notifications of processing essential personal data in connection with the implementation of projects using resources from the European Funds are relatively numerous, the notifying parties are informed about the exemptions applicable to the notification duty (for more information see the Office's website, specifically the column Office's Opinions / Current topics), and as European regulations apply directly to Member States, it is possible to apply the exemption under Article 180(1)(b) of Act No. 101/2000 Coll. in connection with dealing with such projects.

### **Processing of the personal data of passengers by transport companies**

Transport companies in various cities have notified the Office about processing that consists in the installation of camera surveillance systems in public transit vehicles or cameras recording the space in front of the public transit vehicles for the purpose of greater protection of passengers against attacks, protection of property against damage and vandalism, greater safety of passengers and prevention, when using recordings as evidence of crime or inflicted damage or to clarify the causes, and resolving extraordinary events. From the point of view of Act No. 101/2000 Coll., it should be mentioned that the introduction of cameras in all public transit vehicles is essentially not permitted and the principle of proportionality has to be observed and infringement of privacy minimised, in this case the privacy of passengers.

In connection with the activities of transport companies, there are cases of processing appearing that essentially consist in the making of audio recordings during passenger controls. These recordings are intended to provide greater protection to the staff making such controls, as conflicts may arise when dealing with passengers who have breached transport terms and conditions during controls, and to check that the approach chosen by staff during passenger controls was correct. If the records are only used in special cases and not in every situation, no consent is needed for making them under Article 5(2)(e) of Act No. 101/2000 Coll.

### **Breach of personal data protection law (data breaches)**

Upon Act No. 127/2005 Coll., on electronic communications, taking effect, the Office was entrusted with powers related to accepting and assessing notifications regarding data breaches.

In 2014, the Office obtained two notifications of a data breach. The first notification pertained to access being granted to one unauthorised person to files containing the personal data of close to 380 000 customers. With regard to the character of the data and the technical-organisational measures in place and the fact that the data was no longer in the possession of the unauthorised person, the Office took no further measures.

The second notification pertained to the use of the personal data of 300 customers by former partners after their departure from the company. As the notifying party informed the affected subjects, the Office took no further measures.

### **Cloud computing**

The Office has in the last while been receiving notifications of personal data processing via cloud computing. When assessing such notifications, it is important to determine whether the notifying person is in the position of cloud service provider or its customer. As the personal data processing notifications are also made by companies providing cloud computing (cloud services), it should be stated with reference to WP29 Opinion No. 5/2012 on cloud computing (also available in Czech) that the cloud service provided is usually also the data processor. In accordance with Article 16(1) of Act No. 101/2000 Coll., it is always the data controller that files the notification of personal data processing. In this case, it is the cloud computing provider's customer that is the data controller; the data controller is obliged to adopt such measures to prevent the misuse of personal data. With regard to the character of the personal data processing, an exemption to the notification duty can be applied in some cases, e.g., absentee systems, HR etc.



## • TRANSFERS OF PERSONAL DATA ABROAD

Article 27 of Act No. 101/2000 Coll. regulates a special regime for transferring personal data from the Czech Republic to third countries. Third countries are understood in this case to be all countries outside the European Economic Area. The meaning and purpose of this provision is to guarantee protection of personal data of data subjects, where such data is to be transferred and then processed in third countries. Essentially, personal data can be transferred to countries outside the European Union provided these countries guarantee an “adequate level of protection”. An adequate level of protection in a third country can be guaranteed by general legal regulations or sectoral rules of the third country concerned, or such protection can be guaranteed by the data controller (data exporter) itself through corresponding safeguards guaranteeing that level of protection of the transferred personal data will be comparable in the recipient’s country to the protection standards contained in Act No. 101/2000 Coll. Such guarantees may ensue chiefly from the agreement between the data controller and data recipient, where an integral part of such agreement will be standard contractual clauses created by a decision of the European Commission. If the personal data controller chooses the option of creating other kinds of corresponding safeguards, it has to provide “arguments” to defend its own safeguards as part of the permission proceedings under Article 27(4) of Act No. 101/2000 Coll.

Standard contractual clauses intended for use in the private sector and defined by a number of decisions of the European Commission have proven to be the most effective and, in its own way, simplest tool for creating such guarantees.

In the event of transfers of personal data to a personal data processor in a third country, standard contractual clauses that form an annex to EU Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive of the European Parliament and of the Council 95/46/EC should be used.

In the event of the transfer of personal data to a new personal data controller in a third country, it is possible to use either a standard contractual clause contained in EU Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive of the European Parliament and of the Council 95/46/EC<sup>1</sup>; or standard contractual clauses contained in a decision of EU Commission Decision of 27 December amending Decision 2004/497/EC in the case of implementing an alternative set of standard contractual clauses for the transfer of personal data to third countries.

Should the personal data controller conclude an agreement with the personal data recipient in a third country, where standard contractual clauses according to one of the above EU Commission decisions are a part of such agreement, the transfer of personal data will take place according to Article 27(2) of Act No. 101/2000 Coll. “based on a decision of the European Union”. In such case the administrator need not request permission from the Office in accordance with Article 27(4) of Act No. 101/2000 Coll.

Personal data exporters often turn to the Office with the question of whether it is possible to amend the text of a standard contractual clause and under what conditions will an amended clause still be considered a standard contractual clause. If the legal guarantees provided by the



original wording of the clause are preserved, the amended text can continue to be considered a standard contractual clause. At the same time, it should be noted that the Office does not provide opinions that would confirm that the submitted agreement satisfies the particulars of standard contractual clauses.

At Microsoft's request for an assessment of an agreement, WP29, an advisory body to the European Commission on personal data protection issues, took the matter upon itself. This case was shown to be problematic, however, with regard to the fact the WP29 is an advisory body to the European Commission and does not have the authority to issue opinions to private corporations. At the same time, it triggered an avalanche of requests from other corporations for assessment of agreements. Such assessments can only be issued by the various national supervisory authorities. For this reason, the need arose for procedural rules to be put in place for the supervisory authorities on how to proceed in such cases. At this time, WP29 is working on creating a cooperation procedure for assessing whether a presented agreement can be considered a standard contractual clause according to the EU Commission decisions. At this time, one can only say that this procedure is created according to the model cooperation procedure for approving binding corporate rules. It will however be up to companies to decide whether to request a specific supervisory authority to assess the amended standard contractual clauses through this procedure or in some other way; of course, the supervisory authority receiving the request will have the right to refuse to satisfy the request.

The successful application of existing standard contractual clauses intended for the private sector created an initiative leading to the creation of model contractual clauses for the transfer of personal data between public institutions of the European Union and public institutions of third countries. This initiative was embraced by the European Data Protection Supervisor (EDPS). According to this authority's analysis, international agreements usually do not contain European principles of personal data protection; at most, they contain general provisions on adequate personal data protection. The EDPS has drafted model contractual clauses for the transfer of personal data between public institutions in the European Union and in third countries. It is clear that no matter how much a public institution expresses its intention to observe the respective model contractual clauses, they will never be strictly legally binding for the institution, so they cannot become standard contractual clauses in the above sense. The objective of the EDPS is thus to develop through these model agreements general recommendations that the public authorities can follow and that can be used to formulate international agreements.

In the same way that the model contractual clause are being developed, efforts are being undertaken to address cases where personal data is transferred to third countries by the personal data processor, usually as part of the provision of cloud services. At this time, WP29 announced a public consultation to WP29 Working Document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor" (WP 214). The Confederation of European Data Protection Organisations (CEDPO) and the non-profit associations European Digital Rights (EDRi) and European CIO Association (EuroCIO) will participate on this consultation. The draft clauses are based on the specific text of amended "standard contractual clauses" concluded between a Spanish processor and sub-processors in third countries. Based on these clauses and based on the agreement concluded between the data controller and the mentioned Spanish processor, the Spanish data protection authority approved the transfer of data to third countries.

It is understandable that as the European Commission is preparing a new regulation at this time, it has no intention of adopting either the above model clauses for the transfer of personal data between public institutions of the European Union and public institutions of third countries or the model clauses for the transfer of data by European processors to sub-processors in third countries as standard clauses.

Nevertheless, these clauses are another step in expanding European personal data protection standards to hitherto neglected areas.

Until recently, adequate personal data protection in cases of transfer of personal data to the United States of America could also be guaranteed through the registration of the personal data recipient in the United States as an observer of the Safe Harbour principle defined in EU Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

However, when the United States spying programme (PRISM), under which all data of citizens of the European Union were transferred to the US public authorities via Internet companies, was revealed, it raised concerns in the European Union about whether the Safe Harbour principle was in fact able to guarantee the effective protection of personal data in the United States of America.

The European Commission responded to the problems tied to the transfer of personal data to the USA in its Communication to the European Parliament and the Council of 27 November 2013 ("Rebuilding Trust in EU-US Data Flows") and European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)). According to the Communication of the European Commission, many companies on the Safe Harbour list do not observe its principles in practice. Point 38 of the European Parliament's resolution directly states that "as under the current circumstances the Safe Harbour principles do not provide adequate protection for EU citizens, these transfers should be carried out under other instruments, such as contractual clauses or BCRs, provided these instruments set out specific safeguards and protections and are not circumvented by other legal frameworks."

The Office therefore recommends that personal data controllers secure the transfer of personal data to the United States of America, if it proves absolutely necessary to fulfil the stipulated purposes, by way of an agreement that includes standard contractual clauses. These standard contractual clauses at this time indubitably provide a better level of personal data protection in third countries than the Safe Harbour concept.

If the data controller does not address the transfer of personal data to third countries with an insufficient level of personal data protection through standard contractual clauses or in some other way specified under Article 27(2) of Act No. 101/2000 Coll., it has to request permission to transfer personal data to third countries under Article 27(4) of Act No. 11/2000 Coll.

In 2014, the Office received a total of 40 requests for permission to transfer personal data to third countries. The Office adjourned eight cases usually for the reason that the applicant preferred to address the transfer by way of an agreement that included standard contractual clauses.

Of the 30 permits issued in 2014 (two requests are still in process), the most common legal grounds based on which the Office issued the permit was Article 27(3)(b) of Act No. 101/2000

Coll., as the applicant created sufficient special personal data protection guarantees in the third country always through approved Binding Corporate Rules (BCRs). This occurred in 18 cases. BCRs were discussed in relative detail in the Office's 2013 Annual Report. In seven cases, the legal grounds for the permit was Article 27(3)(a), i.e., the transfer of personal data upon consent or based on the instructions of data subjects. In four cases, the legal reason was Article 27(3)(e), i.e., the transfer of data necessary for negotiations on the conclusion or amendment of an agreement at the instigation of the data subject or for the performance of an agreement to which the data subject was the contractual party.

Geographically, the transfer of personal data concerned, as usual, the following countries: USA, India and South-East Asia and the Pacific (Japan, China, Philippines, Australia) and (in two cases where travel agencies were concerned) Turkey and Egypt.

## • SCHENGEN COOPERATION

Just like in previous years, in 2014 the Office actively took part in operations tied to supervision in the area of Schengen cooperation, chiefly supervision over sharing personal data in international information systems. In its position as the supervisory authority for the Czech Republic, the Office supervised the observance of the relevant legal regulations, primarily for the purpose of protecting the personal data of subjects whose data is processed within the Schengen area. The second generation Schengen Information System (SIS II), which eliminates the security risk tied to the free movement of persons and things inside the Schengen area, holds a pivotal position among information systems on the European level. Supervision over the proper processing of personal data in the Visa Information System (VIS), Customs Information System (CIS) or EURODAC (international fingerprint database for identifying asylum seekers and irregular border-crossers) is also included among the Office's duties.

With regard to the above, the Office tackled this topic as part of its supervisory activities on the national level and as part of meetings of the respective working groups that included representatives of the various EU Member States or states contributing to the utilisation of the respective information system.

### • Inspections of information systems and the results thereof

As processing the data of subjects in the above systems can potentially threaten such subjects' rights, including the right to the due processing of personal data, the Office focused on the systematic examination of the information systems concerned. In 2014, a national inspection focusing on the transition to the second generation Schengen Information System was thus carried out. The inspection examined in particular the observance of all security aspects of operations carried out by the Police of the Czech Republic, as the authorised personal data controller in the national part of the Schengen Information System, with the personal data of subjects.

The findings from the inspection and the documents requested helped to ascertain the state of affairs. This was followed by a legal assessment of the transition from SIS 1+ to SIS II and of the procedure for handling a request of a specific person and by an examination of the way the personal data of such person was processed in the SIS. The legal assessment was based on the appropriate national legal regulations in the field of personal data protection and on binding EU regulations regarding the processing of personal data in information systems operated under Schengen cooperation. The inspection found no breach of Act No. 101/2000 Coll. Thus no Remedial measures were imposed. In her conclusions in the inspection protocol, the Office's inspector recommended drawing up an updated security study of the national part of SIS II and of the body responsible for it (Presidium of the Police of the Czech Republic), so that when processing requests it would search for the personal data requested in the application directly in the system and then document the results in the file to allow for the procedure to be reviewed, including preserving information about the personal data of the queried based on a request in the national part of SIS II.

The Office further examined the activities of the Ministry of Foreign Affairs as one of the personal data controllers in connection with the processing of personal data in the Visa Information

System (“VIS”) also by inspecting the Embassy in Cairo. The purpose of the VIS is first and foremost the exchange of visa data between member states with the aim of improving the implementation of common visa policy and consular cooperation. Although the inspection did not ascertain any breach by the Ministry of Foreign Affairs of its obligations under Act No. 101/2000 Coll., the Office nevertheless called attention to the problematic aspect of personal data processing. The main focus was on the use of outsourcing services provided by private companies. The companies concerned accept Schengen visa applications which includes scanning the fingerprints of applicants from remote areas of territorially large countries and then distributing the data together with personal and sensitive data to embassies operated by the Czech Republic. The Ministry of Foreign Affairs is involved in the activities of these so-called visa centres in the Russian Federation only. During the inspection, it was revealed from open sources the intention to expand the mentioned cooperation with private companies to other countries, specifically China and North African countries. As the mentioned companies are in the position of personal data processors, the Ministry of Foreign Affairs has to agree to the strict observance of the obligations under Section 6 of Act No. 10/2000 Coll. and conclude a personal data processing agreement with each of these companies. The greatest amount of attention has to be paid to guarantees by the processor concerning the technical and organisational safeguarding of the personal data processed in VIS and subsequent controls.

Last but not least, an inspection was conducted of the Customs Information System, the purpose of which is to help to avoid, investigate and reveal operations that are at variance with customs or agricultural regulations of the European Union or are in serious breach of the national regulations of EU Member States. A special database – Customs File Identification Database (FIDE) – is part of the Customs Information System. It is possible to review the results of the inspection in the section of the annual report on the results of the Office’s supervisory activities.

#### • Judicial rulings

The Office systematically provided information about activities and news in relation to Schengen cooperation, e.g. by arranging an information campaign. Although acquainting the respective authorities took place without any problems, certain shortcomings were registered in connection with the awareness of both the general public and professions about certain procedural aspects of data processing in information systems. The above is evidenced chiefly by the latest judicial rulings of the Supreme Administrative Court.

In its ruling of 25 June 2014, ref. no. 1 Aps 15/2013-33, the Supreme Administrative Court stated, inter alia, the following: “If a person about whom a record is kept in the Schengen Information System (SIS) does not agree with such record, he or she must first file a request for deletion or correction of such record from SIS with the Police of the Czech Republic, specifically the Police Presidium (Section 84 of Act No. 273/2007 Coll., on the Police of the Czech Republic). The fact that the record was not entered in the Schengen system by the Czech side but by some other state has no bearing on this procedure (Article 106 of the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders). The Police of the Czech Republic is obliged to do all in its powers to delete the applicant’s data should the data in SIS be kept at

variance with the law [Article 106(3) and Article 115 of the cited convention] This shall apply despite the fact that the Police of the Czech Republic is not responsible for the data being accurate and up-to-date (Article 15 ad idem).” The case concerned a request filed by the complainant that the Police of the Czech Republic delete an alert pertaining to him in SIS II although the alert was issued by a different Member State. He then filed a request with the Office for deletion of the alert in SIS II, although based on the relevant legal regulation neither the Office, nor the Police of the Czech Republic nor any other Czech authority is the competent authority. Article 34(2) of the SIS II Regulation (formerly Article 106(1) of the Convention implementing the Schengen Agreement) explicitly states that only the Member State that issued the alert shall be authorised to modify, add to, correct or delete data which it has entered. With regard to the above, no Member State of the European Union, and thus not even the Czech Republic, has the authority to delete an alert that a body of a different Member State issued in SIS II. Nevertheless, the Office contributes to spreading information about issues related to personal data processing in information systems. In the coming years it will continue to work on increasing the general public’s and professionals’ awareness of Schengen cooperation.

- **Number of instigations, complaints and queries and their processing**

During 2014, the Office obtained a total of ten instigations regarding personal data processing in SIS II. The subject of the requests was chiefly the provision of information about the processing of personal data of applicants in the national part of SIS II, and the handling of requests for correction or deletion of the personal data processed therein. A number of instigations were aimed at reviews of negative decisions in Czech visa proceedings or Czech residency proceedings. In one case, the Office was asked to cooperate with the French supervisory authority in the matter of an alert that the respective Czech authority entered into SIS II. As in previous years, the Office cooperated with the Police of the Czech Republic on these cases.

As concerns the visa policy of the Czech Republic, the Office continues to register numerous queries and requests that fall within the purview of the Ministry of Foreign Affairs. The number of such cases in 2014 was 66. When processing these instigations, the Office first clarified the jurisdiction of the authorities in the visa sector, provided information about the possibility to contact the Ministry of Foreign Affairs and then explained its own supervisory powers.

# LEGISLATIVE ACTIVITIES

In 2014, the Office was affected by two new legal regulations:

The procedural amendment of Act No. 101/2001 Coll., effective from 1 May 2014, adopted in connection with the new Control Code, brought the hitherto procedural rules for controls of personal data protection in line with the new procedures under the Control Code, while making provisions for the definition of independent supervisory authority stipulated by Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The amendment deleted all provisions that were assessed as duplicate under the Supervision Code. Act No. 101/2000 Coll., however, retains the express statutory authority of inspectors to have access to all required information, especially information protected by special regimes where special rights of access are not addressed by the Supervision Code. This authority is based on Directive 95/46/EC, which demands that supervisory authorities have access to data that is subject to processing and the authority to collect all information that is necessary for them to fulfil their supervisory role. Using other supervisory authorities as a model, the power to consider whether and in what situations it is possible to waive fines for breach of obligations when processing personal data was added to the law. The amendment finally set the rules for supervisory procedures pertaining to personal data processing running in parallel with other supervisory procedures – preliminary assessment of processing reported to the Office pursuant to Article 16 of Act No. 101/2000 Coll.

The amending legislation building on Act No. 234/2014 Coll., on the civil service, included the Office in the list of central administrative authorities. Along with this, Article 2(2) of Act No. 101/2000 was amended, and with effect from 1 January 2015, it stipulates that the Office is the central administrative authority for personal data protection to the extent set out by Act No. 101/2000 Coll., special legal regulations, international agreements that are part of the law and the directly applicable laws of the European Union. The civil service rules will have implications for most Office employees. The President of the Office is a service body and is authorised to instruct civil servants to execute civil services according to Act No. 234/2014 Coll., the Civil Services Act. The Civil Services Act expressly states that it does not apply to the President and inspectors of the Office; however, it has not fully resolved the relationship of the Office, as an independent supervisory institution, to the government.



According to Article 28 of Directive 94/46/EC, the Office shall act with “complete independence”. Although the independence of the Office is declared in Article 28 of Act No. 101/2000 Coll., the provisions of a jurisdictional law that, inter alia, impose tasks on central authorities do not distinguish a group of independent supervisory authorities not subordinated to the government. This longstanding problem may only be resolved by a new jurisdictional law.

In the field of consultation of legal regulations, the very popular disclosure of personal data with the declared objective of transparency of public administration and the fight against corruption is a new addition to the problematic personal data processing issues and trends from previous years, such as the assessment of the impact on privacy and the development of new government databases. With regard to this trend, the Office called attention to an appropriate and reasonable way of disclosing data and to the statutory requirement that the state work with data in a structured and effective manner, as well to the fact that in numerous cases not even the continuous or subsequent disclosure of data from public administration, including personal data, can take the place of missing standards and control rules.

The Office provided consultations on the contemplated amendment of Act No. 159/2006 Coll., on conflicts of interest, that would introduce a centralised overview of notifications under Act No. 159/2000 Coll. and on the methods of making information from such a register available to the public. The explanatory memorandum to the amendment has to clearly explain what selected, law-given criteria for processing and disclosing data is considered by the State to be the most effective for satisfying the purpose of Act No. 159/2006 Coll. The data that is to be available (without restriction) to the public in the central register should be defined exactly. Under Act No. 101/2000 Coll., it is already possible to disclose a host of data on the activities of civil servants. Conversely, the Office considers the option where all detailed information and documents from the registry of civil servants is published on the internet in unrestricted form to be highly problematic also with regard to the judicial rulings of the Court of Justice of the European Union regarding the conflict between the right to information and the right to privacy, especially in the cases of *Rechnungshof v. Österreichischer Rundfunk* and *Schecke and Eifert v. Land Hessen*. Current is also the debate on the method of implementing the “right to be forgotten” on the Internet, which has now been defined by the Court of Justice of the European Union in the matter of *Google v. Costeja*.

In a number of cases of fundamental or extensive legislative changes, the Office registered the intent of the responsible ministries to submit draft amendments of legal regulations directly without drawing up an objective, providing a detailed analysis of the issue and assessing the alternatives to the possible scope of the legal regulation. This approach does not relieve the ministries of the obligation to address personal data protection aspects before drawing up the various sections of the amendment.

In the case of the amendment of Act No. 561/2004 Coll., the Education Act, that is to introduce a teacher registry, the Office called attention to the obligation stipulated by the legislative rules of the government to assess the impact that the planned registry would have on privacy.

This means that the Ministry of Education, Youth and Sports is required to describe and assess the possible variations of the registry: a decentralised one that allows access to aggregate data from schools and would allow the ministry to obtain current statistical overviews regularly; and a national, centralised one which stores data about teachers and other educational workers and would allow one to work with data monitoring the entire careers of teachers. The

option that includes the central collection and storage of personal data from school information systems, which also means a greater infringement on privacy, in particular requires a thoroughly drawn up justification of the need of the register for planning (staffing) of schools.

The objective of the law was sorely lacking in the case of the draft of the new gaming law submitted for consultation by the Ministry of Finance. The material submitted did not duly describe the purpose or the objective of the register of individuals prohibited from taking part in games of chance, nor was the legitimacy and proportionality of the personal data processing assessed. Furthermore, the Office called attention to a possible conflict between legal regulations and the banning of people carried out exclusively based on the automated processing of personal data, where the entry in the register would only be based on other legal facts, i.e., if a person received social benefits or filed for bankruptcy. The above is a case of sweeping and discriminatory solution. It is the Office's opinion that a decision about each person can be made individually based on the given criteria or for a stipulated period and in a specified area. The Office further called attention to the unconstitutionality of the whole solution, as such automated measure should have been eliminated by a proper administrative review.

The material also insufficiently discussed the mechanisms for processing the personal data described in the part pertaining to filling the record of banned persons with data (or the method of transferring data from the Ministry of Labour and Social Affairs), the justification for the Ministry of Finance maintaining the record and the division of access to the record. The short sentence in the explanatory memorandum justifying the identification of individuals in a gambling house or casino by claiming that mandatory identification represents "social protection" of the betters is not considered to be sufficient reason for infringing on privacy. The draft submitted for consultation also did not clarify in any way whether and how the legal regulation (in its draft form) intends to address monitoring.

As the explanatory memorandum to the draft law did not contain a description of a majority of the basic particulars of personal data processing, the Office raised a number of important comments in the consultation procedure at the end of the year. What is illustrative is that the Ministry of Finance "boasted" that it had consulted the Office in May of that year and yet did not reflect in the material a single standpoint that the Office had presented to the ministry's representative at this meeting.

In 2014, the Office also provided its opinion on Act No. 106/1999 Coll., on free access to information, where it also proposed clarifying the disclosure of data on salaries, about which the courts have recently be ruling on in a fundamental way, by stipulating statutory thresholds so that municipalities would not be burdened in their day-to-day practice with performing proportionality tests when weighing public interest and protection of privacy. The Office therefore proposed to the Ministry of Interior that Sections 8a and 8b of Act No. 106/1999 be specified.

The Office also opined on the possibility of establishing an information commissioner or entrusting this role to some office. The Office expressed its conviction that such an authority would be beneficial as it is clear from the many consultations handled by the Office that accountable entities, especially municipalities, are helpless in this matter. A methodology and advice on access to information could at least help them avoid breaching the law. At the same time, it ensues from an analysis performed by the Ministry of the Interior that the role of an information commissioner is quite common in other European countries.

One of the less frequent cases of legislative work is providing comments to draft amendments of legal regulations during inspections conducted by the Office. The Office was presented with a draft decree on medical records that would introduce a new form of card with new-born screening. The Office did not dispute the need for new-born screening and the necessary administration tied to this process. It did, however, warn that the methodological guideline of the Ministry of Health based on which the procedure had hitherto been implemented is not a sufficient legal regulation for fulfilling the statutory purpose and for the further retention of data. The processing of personal data is only possible based on the express legal regulation and no other kind of regulation justified further processing, including the storage of samples, in excess of the original purpose of processing. For this reason, the Office suggested that the legal grounds and the periods of further storage and processing of blood samples be further clarified.

The Office also noticed that the amendment to the new Civil Code would also have an unexplained impact on privacy. The amendment would have required the entry of certain data about certain individuals involved in the operation of trust funds into a trust fund register. The Office did not consider the claim that “all in all, any implications would not be excessive” to be substantiated.

The Office assesses positively the offence register, the statutory form of which had long been thoroughly prepared and discussed, and the resulting form of the legal regulation testifies to this. In relation to the protection of privacy and specific personal data, an acceptable solution was found in connection with the search for a balance between important social interest in protecting all and individually defined rights and interest in the protection of personal data. Certain offences under Act No. 200/1990 Coll., on offences, will be monitored – i.e. recorded and taken into account when heard; recidivism will be prosecuted and for the purpose of assessing the credibility of individuals, offences under special laws will be recorded in addition to certain offences under Act No. 200/1990. At the same time, it was possible to achieve such a definition of conditions that access to the register should be sufficiently restricted and tied to a clearly specified reason. Access to data by authorised bodies is strictly tied to the need for such data in order to fulfil a specific task in line with their powers and does not authorise them to use the data if not necessary in the case at hand.

The Office was exceptionally allowed to comment on the amendment of a legal regulation that is not subject to its supervision. This regulation concerns supervision over the processing of personal data obtained from intelligence services. The Office called attention to the insufficiency of the regulation as the current statutory form of control precludes the use of standard supervisory powers in connection with the processing of personal data but at the same time it is not possible to attain a comparable degree of control through permission granted by the court for each case and not even the existing model of control by the Parliament of the Czech Republic does not correspond to the needs of effective control. The need for a permanent and competent supervision over personal data processing exists if only for the reason that intelligence services are allowed to process the personal data of an extraordinary number of people and such data is primarily processed for other purposes and it is not possible for the affected data subjects to anticipate or prevent its secondary processing. In addition, the possibility of data subjects to meaningfully fulfil their rights is precluded under existing legal regulations.

# FOREIGN AFFAIRS AND INTERNATIONAL COOPERATION

The field of foreign cooperation in personal data protection was influenced in 2014 by intensive discussions about the monitoring of the electronic communications of the world's citizens (the topic of a "post-Snowden" world) and by a number of decisions of the Court of Justice of the European Union in Luxembourg directly pertaining to personal data processing under European Directive 95/46/EC. Both had certain implications not only on the practice of national supervisory authorities but also a substantial influence on the still unfinished preparation of the new European personal data protection regulation. In a number of cases, the global nature of personal data protection is becoming clear and so it is natural that even for this reason key issues and current supervisory trends in the field of personal data protection have recently often been dealt with in tandem on the pan-European level within the advisory body of the European Commission, the Article 29 Data Protection Working Party (WP29).

WP29 sessions are regularly attended by the President of the Office and other representatives of the Office working in certain topics on the WP29 subgroups. In 2014, the opinions of WP29 focused on the topics of data breaches, anonymisation techniques on the internet and dactyloscopic equipment. The opinions are usually drawn up based on findings shared by supervisory authorities and consultations with stakeholders; nevertheless, own research was carried out under the WP29 Technological Subgroup on the use of cookies on the websites of internet media, the private sector (especially e-shops) and even public administration. Representatives of the Office took part in the creation of the methodology and selection of the scope of the research and in their own research. The data acquired on behalf of the Czech Republic is represented in the resulting report. The Office also actively contributed to a number of WP29 documents for personal data processing in special areas of the enforcement of rights and monitoring electronic communications for national security purposes as well as to opinions on rescinding the long-criticised

European Data Retention Directive. Most technical meetings built on the WP29 meeting in 2014, where the representatives of the Office presented practical experience or positions of the Office on the civil use of drones (meeting organised by the European Commission) or on the surveillance of public space using cameras and copying documents as part of the fight against money laundering (26th meeting of the representatives of data protection authorities, Case Handling Workshop).

Above and beyond the framework of opinions and working documents, the WP29 plenary session at the end of the year focused on the need for a broader debate about the future of privacy protection and about preserving European personal data protection values by emphasising the need to promote European privacy protection values especially with regard to the advancing digitalisation of everyday life (<http://europeandatagovernance-forum.com>).

The Office took part in developing common knowledge basis for WP29 in response to a decision of the Court of Justice of the European Union in reference for a “preliminary ruling” in C-131/12 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González. The court ruled that “An internet search engine operator is responsible for the processing that it carries out of personal data which appear on web pages published by third parties” and confirmed the existence of the right to delete search results (right to deletion, right to de-listing or the right to be forgotten) also in the environment of the internet and especially in the environment of an internet search engine. Whereas the Office on the national level issued a recommendation following discussion with industry representatives, in the matter of the procedure vis-a-vis global internet search engine operators, established as personal data controllers in a different Member State of the European Union, it coordinated a common approach and exchange of information with other supervisory authorities, the result of which was a joint document of WP29 discussing the application of the conclusion of the court judgement.

Another current decision of the Luxembourg court on personal data protection affected the Office directly. In the matter of Case No. C-212/13 František Ryneš v. Úřad pro ochranu osobních údajů, a representative of the Office appeared at the hearing of the Court of Justice of the European Union and argued the opinion of the Czech Republic (government) regarding exemption of certain kinds of camera systems from personal data protection rules. In the subsequent decision, the court agreed with the opinion of the Office that “the personal data protection directive applies to a video recording made using a camera system installed by a person on their family home but which also monitors public space” and that “to the extent that video surveillance covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely ‘personal or household’ activity”.

Since January 2012, the Office has been involved in negotiating a new European legal framework for the protection of privacy and is regularly commenting the draft position of the Czech Republic (government) in such negotiations. Similarly, the representatives of the Office worked on modernising the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data at the T-PD Committee and the Ad Hoc Committee on Data Protection (CAHDATA).

In recent years, the Office most often encountered opinions of the representatives of the Government of the Czech Republic that diverged from the long held views on personal data

processing principles both on the level of the European Commission and in cases heard by the Court of Justice of the European Union. A typical example was the Czech Republic's requirement at the end of the year for limiting the force of Convention No 108 although during earlier harmonisation efforts the system of existing exemptions for special processing of personal data was sufficiently explained and broadly accepted. For this reason, the Office appreciates the opportunity for cooperation when the Ministry of Foreign Affairs is requested to provide its opinion in judicial preliminary rulings, and can contribute in a timely manner and influence the wording of a joint standpoint.

One of the important cases of 2014 that the Office could opine on was the Case 362/14 (Schrems). The essence of the case is the claim that there is no substantial protection of personal data transferred to the USA in the laws of the USA and in practice. Because of doubts about how to interpret European law in the case at hand, the Irish court decided to ask for a preliminary ruling from the Court of Justice of the European Union on the issue of transferring personal data to third countries under Article 25 of Directive 95/46/EC. Personal data in compliance with this article can be transferred to third countries if third countries provide a corresponding level of protection of personal data. The European Commission had formerly acknowledged that the USA satisfied this protection and Member States of the European Union are bound to the decisions of the Commission based on Article 25(5) of Directive 95/46/EC and can no longer decide on this issue by themselves. Let us hope that the decision of the Luxembourg court on the preliminary issue can be a fundamental contribution to the debate between the EU and the USA on the transfer of personal data and a breakthrough in the issue of data transferred between the EU and the USA for the purpose of promoting rights (prevention, investigation and prosecution of crime, including terrorism) about which the European Union has been conducting negotiations with the government of the USA since Spring 2011.

In addition to cooperation on the central level, the Office has been developing bilateral relations and continues with projects with partner offices. The Office completed cooperation with partners from Poland, Bulgaria and Croatia on the project "Raising awareness of the data protection issues among the employees working in the EU" financed from the EU's Lifelong Learning/Leonardo da Vinci – Partnership programme. The project was aimed at common European principles and rules for personal data protection on workplace privacy. The primary output is a handbook intended chiefly for employees. Employers, trade unions and recruitment agencies were also interested in this publication.

Of the new offers for cooperation, the Office accepted an offer from its Bulgarian colleagues to prepare projects aimed at protecting children. The Office met with its Slovak colleagues in the middle of the year for a full-day meeting. As part of the project entitled "Putting law into practice and practice into law" ("Právo do praxe, praxe do práva"), which the Office is working on with the Law Faculty of Masaryk University in Brno, the Office accepted a study visit from DePaul University in Chicago.

In November 2014, the Office co-organised an international workshop on the issue of personal data processing in connection with detecting and investigating fraud in the employee sector. Representatives from supervisory authorities for data protection from eight European countries (Poland, Estonia, Macedonia, Montenegro, Albania, Romania, Bosnia-Herzegovina and the Czech Republic) as well as representatives of Czech and international companies active in this issue attended this workshop. The discussion pertained very much to the legal

conditions of investigations in the context of the protection of the rights of the investigated employees. Whistleblowing was part of the programme of the workshop.

Representatives of the Office continued in 2014 as well to work in special European control groups (and coordination groups for supervision), in Europol, the Schengen Information System, the Visa Information System, the Customs Information system and the EURODAC system as well as in the Schengen evaluation group.



# OFFICE, MEDIA AND COMMUNICATION TOOLS

The Office continues to regularly inform the public about its current efforts via its revamped website. Responses to questions from reporters were provided as soon as possible, usually on the same day but no later than within three days. Questions from reporters often became the impetus for inspections conducted by the Office or for supplementing factual materials as well as the trigger for control activities or administrative proceedings. In such cases, synergy of the work of the Office with information from public sources occurred and can be expected to continue due to the ever growing knowledge of personal data protection and concerns about the loss of privacy.

It is clear that even fourteen years after personal data protection was enshrined in the law it is not possible to give up on raising awareness about personal data protection as a distinctive attribute of democracy and it is necessary to continue to promote the values tied to the protection of privacy. In cases where a more subtle approach need to be taken – for example in the case where it is necessary to weigh the protection of privacy against public interest – it is apparent especially on the part of some reporters the clear preference to publish information without greater forethought. Ignoring the need for the balanced application of the right to privacy and access to information is often facilitated by the publication of opinions that do not believe personal data protection to be necessary.

An overview of the activities of the Office, the most followed cases as well as the most serious issues tied to personal data protection are systematically made available on the website of the Office in the columns “Press releases and conferences” and “Opinions”. The following positions of the Office are also available here: Position No. 1/2014 - Smart metering and protection of personal data; Position No. 2/2014 - Dynamic biometric signature from the point of view of the Personal Data Protection Act; Position No. 3/2014 - Regarding excessive demands for approval of personal data processing and the related incorrect fulfilment of the notification duty; and Position No. 4/2014 - Transparent Accounts and Personal Data Protection.

## RAISING AWARENESS ABOUT PERSONAL DATA PROTECTION

On the occasion of Personal Data Protection Day set for January 28, the Office announced the 8th annual “My Privacy! Don’t Look, Don’t Snoop!” (“Moje soukromí! Nekoukat, nešťourat!”) contest. This year, the contest aimed to call attention especially to the fact that no one knows



for certain what will happen to information once placed on the internet. The objective will be to spark the interest of children and youth in this issue especially as most are daily users of the internet and social networks. The results of the contest were announced in the presence of the accompanying teachers. The usual practice is to hold preliminary rounds in participating schools, with only the best works then being sent to the Office. It is apparent that teachers truly know how to make use of this activity and share knowledge that can be offered in an entertaining way to the benefit of a wider group of students than just the most successful and most agile. This is certainly promising for the inclusion of personal data protection in the computer literacy curriculum. Contributions from the competition are published permanently on the Office's website and the best artwork was used to create items promoting responsible behaviour on social networks (pins that youth like to wear on their backpacks).

As a show of appreciation for taking part, the Office gave all participants the publication entitled *Web We Want*, which was published with support from UPC, from whom the Office received the issues for contest participants as a gift at the conference of the Czech Association of Electronic Communication, which was organised under the auspices of the President of the Office.

The interest of law students in personal data protection was shown by the request of ELSA Prague to meet with experts. The seminar about European and domestic legal documents and even specific casuistry was attended by the students, who filled the meeting rooms offered by the Office and showed great interest by being active in discussions.

As is the case each year, the staff members of the Office gave lectures at a great number of seminars and conferences for government institutions, local governments and even private businesses.

Round tables have become the main form of communication with experts about the work of the Office, such as the round table on the topic of Intelligent Networks and Intelligent Measurement Systems and Equipment in the Context of Conditions for Personal Data Processing, which was organised in cooperation with the Ministry of Industry and Trade. The discussion was also attended by the representatives of other stakeholders, chiefly from the ranks of producers and suppliers of energy as well as companies involved in billing energy supplies, the energy market operator and representatives of producers and distributors of the respective technological solutions and representatives of academia.

A seminar with international participation (Albania, Bosnia and Herzegovina, Montenegro, Estonia, Macedonia, Poland and Romania) on the topic of personal data processing with detection and investigation of fraud in the employee sector and the issue of whistleblowing was held at the end of 2014. The law firm bnt attorneys-at-law co-organised the seminar.

## OFFICE LIBRARY AND PUBLICATIONS

The Office Library continues to be primarily used by Office employees but also by students for their papers and theses on personal data protection.

In 2014, this highly specialised library acquired 38 new titles and received 5 titles as gifts.

The Office also began issuing its own official Journal exclusively in electronic form. This publication continues to be intended for experts. In addition to the particulars imposed on the

Office by law, which is an overview of cancelled registrations, the Journal contains the Office's standpoints, legal analyses, information about the decisions of the Office and the results of certain inspections conducted by the Office. It also contains important discussions on events in society that in some way are related to personal data protection. Document of an international nature are also an important part of the Journal.

In 2014, an issue of the Information Bulletin was published that provided information about the round table that was held and about the opinions that were heard on the issue of smart measuring. It however focused on clarifying the process of receiving and handling instigations and complaints by the Office in the effort to inform the general public about the procedures that it can use if it encounters problems with personal data protection.

In 2014, the Office – in conjunction with its partner offices in Poland, Bulgaria and Croatia – published a brochure on the protection of personal data of employees at the workplace. The two-year project was officially concluded by presentation of the publication to the public. Office President Mr Igor Němec invited representatives of the embassies of the partner countries as well as representatives of recruitment agencies, trade unions, the work inspection offices, law firms and the media. The publication was met with acclaim especially by recruitment agencies, trade unions but also by certain professional periodicals, which expressed interest in using the publication in their sphere of action. The publication was also well received by foreign colleagues from the Romanian office for personal data protection, which expressed interest in having it translated into Romanian. The outcome of the project is permanently available to whomever is interested in the Publications column on the Office's website.

## OFFICE WEBSITE

The Office's website has change both in terms of graphics and in terms of user friendliness and breadth of educational possibilities. This occurred on the occasion of the transfer to work with an editing system. The main user-relate change is the possibility since the beginning of the year to search for a specific topic (e.g. health care, education, public administration) or various legal provisions, sections of Act No 101/2000 Coll. among other things. This possibility, available directly from the homepage of the website, facilitates and accelerates access to basic documents on the issue in question. The statistics on visits to the various pages of the website showed that the general public is most interested in camera surveillance systems, which was confirmed by the popularity of the Camera Surveillance Systems column under the Consulting Room section on the homepage.

# ORG INFORMATION SYSTEM

The ORG Information System, which creates and submits “agenda” identifiers from one agenda to another and keeps a list of them, is part of the “Information System of Basic Registers”. This system was created on the basis of Act No. 111/2009 Coll., on basic registers, and is used primarily by the public administration authorities. It facilitates communication between people and the authorities. It operates 24 hours a day, seven days a week.

Testifying to the fact that the system is growing day by day, requests are being sent to the National Registers Authority (the “NRA”) on a daily basis for the creation of new links between the agenda and information systems of users. Each information system of a user has to be certified by the NRA and entered into the system. As at 31 December 2014, 377 agendas and roughly 72 000 links to the information systems of end users were entered into the system. Large and well-known agendas include e.g., Social Security, Healthy Insurance, Driver Registration. However, Hop Protection, Anti-Drug Policy and Support for the Film Industry can also be found among the agendas.

The system load (number of transactions) changes during the year, but even such a big event as the municipal elections this year did not burden the system as much as the presidential election in 2012, when a lot of data in the system was verified, supplemented and updated.

The DRP (Disaster Recovery Plan) is tested regularly. The test confirmed that the system would continue to operate even if one data centre failed.

The effectiveness of such training and testing of the transfer to a backup centre was verified in connection with a real power failure of the data centre connected at the time. The transfer to the backup data centre took place in the stipulated period of time and without any loss of data.

The operation of the ORG IS is monitored by the Service Desk Application run by the NRA. Here all operational requirements and events related to operation, testing and expansion of the system are recorded.

In 2014, the audit commenced in 2011 by an entity authorised by the Ministry of Finance and Ministry of Regional Development was completed. The standpoint issued by the Prague Tax Office in the audit stated that no shortcomings were found in the financing or implementation of the “ORG Information System in the Basic Registers System” project.

# OFFICE PERSONNEL

The number of positions at the Office is determined by the state budget and has been set at 102 since 2010. Compared to the previous years, the employee fluctuation rate fell from 10% to just under 6%. Employment contracts were concluded with six new employees, with two being concluded for a definite period time to cover the maternity leave of two employees. Four employees left the Office, one of which due to retirement.

As at 1 January 2014, the Office had 99 employees; as at 31 December 2014, the number was the same. The average converted number of employees for 2014 was also 99.

An addition 28 employees worked for the Office based on an agreements concluded outside of an employment relationship. Nineteen Agreements to Perform Work were concluded in connection with work requiring longer commitments, such as membership in the Appeals Committee of the Office, help with the ever growing number of work-relate tasks, especially in connection with Act No. 480/2004 Coll., on certain information society services (unsolicited commercial communication), consultation work and drafting of internal regulations. A total of nine Agreements to Complete a Job were concluded for short-term projects, such as lecturing or assessing the contest "My Privacy! Don't Look, Don't Snoop!" ("Moje soukromi! Nekoukat, neštourat!").

It ensues from the table "Office Employees Divided According to Age and Sex" that mainly employees aged 50 and above (54%) work at the Office. In addition to the corresponding education and long-term professional practice and extensive experience, the majority have been employed at the Office since its establishment and have passed on their experience to new employees, usually university graduates who are hired to fill vacant positions. A university education is required for two-thirds of the positions at the Office. The remaining third requires a secondary school diploma. The table "Office Employees Divided According to Age and Sex" clearly shows that the employees of the Office fulfil the education criteria to perform their jobs.

# ECONOMIC MANAGEMENT OF THE OFFICE

The budget of the Office was approved by Act No. 475/2013 Coll., on the State budget of the Czech Republic, for 2014.

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

in CZK thousands

### Summary indicators

Total income	2 677.80
Total expenditures	124 767.14

### Specific indicators – income

Total non-tax and capital income and accepted transfers	2 677.80
of which:	
total income from the budget of the European Union. excl. CAP	702.54
other non-tax and capital income and accepted transfers in total	1 975.26
other non-tax and capital income and accepted transfers in total	1 975.26

### Specific indicators – expenditures

Expenditures to ensure performance of the tasks of the Office for Personal Data Protection	124 767.14
--	---------------

### Cross-cutting expenditure indicators

---

Salaries of employees and other payments for performed work	44 743.48
Mandatory insurance premiums paid by the employer*)	15 143.04
Contribution to the Cultural and Social Needs Fund	432.76
Salaries of employees within an employment relationship	35 179.95
Salaries of employees derived from salaries of constitutional officials	8 032.78
Total expenditures co-financed from the budget of the European, excl. CAP	193.23
of which:	
from the state budget	0.00
contribution from the EU budget	1 93.23
Total expenditures recorded in the information system of programme financing EDS/SMVS	7 210.05

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

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

In 2014, the Office received a total of 74 requests for information. This number is comparable with the previous year, which confirms the public's interest in the work of the Office or in personal data processing as such.

Of the total number of information requests, the Office fully satisfied 43, partially rejected 23 and fully rejected 8 in 2014. The most frequent reasons for the partial or full rejection of information requests included protection of the personal data contained in the information requested, especially protection of the data pertaining to third parties, injured parties or witnesses in proceedings conducted by the Office, and protection of information obtained during inspections, such information being protected by the law and subject to confidentiality. The average time it took to handle one request for information in 2014 was six days. The statutory 15-day deadline for handling information requests was not exceeded in any case.

There was one decision on partial or full rejection of a request for information that was contested using a due remedial measure, i.e., through appeal procedure. The President of the Office, as the appellate body, did not satisfy the appeal, thereby confirming the Office's approach to handling the request for information in this case. The subject of the proceedings in this request for information was access to the full file of an applicant who was not a party to the proceedings or interested in reviewing the file. In compliance with the decisions of the administrative courts, which consider the regulation on reviewing files according to the Code of Administrative Procedure in conjunction with Act No. 106/1999 Coll. to be a special legal regulation, this request was dismissed. The procedure for handling requests for information was also contested in a complaint under Section 16a of Act No. 106/1999 Coll. The subject of the complaint was the fact that the petitioner for the information was not sent one of the requested documents although he was entitled to it. This error was rectified immediately.

The Office's approach to handling information requests under Act No. 106/1999 Coll. was not under judicial review in 2014 as well. The Office thus did not incur any related costs.

In term of content, the requests for information most often concerned the court decisions and the judicial review thereof. The petitioners either requested inspection conclusions or administrative decisions concerning certain categories of data controllers or certain activities, information about judicial review of the Office's decisions including the administrative actions themselves and the Office's response to them or more information in the case of proceedings commenced by the Office based on a prior instigation. An insignificant number of requests for information related to the Office's financial management. It is standard for the Office to publish the content of the provided information for other users on its website.



# COMPLAINTS PROCEDURE UNDER SECTION 175 OF THE CODE OF ADMINISTRATIVE PROCEDURE

In 2014, the Office again dealt with complaints under Section 175 of the Code of Administrative procedure based on the petitions from the aggrieved parties who have the right under this provision to turn to an administrative authority with a complaint if they believe that the administrative authority proceeded incorrectly or if a public servant behaved in an inappropriate manner. This recourse under the Code of Administrative Procedure serves to protect the rights of aggrieved parties if the law does not provide them with any other means of protection.

In 2014, the Office handled a total of 39 complaints that were assessed and handled as complaints under Section 175 of the Code of Administrative Procedure, of which 10 were assessed as warranted and 5 as partially warranted. The remaining 24 were found to be unwarranted. In comparison with the previous year, the total number of complaints remained about the same.

The statutory period for processing complaints under Section 175 of the Code of Administrative Procedure is 60 days. In 2014, the Office processed complaints on average within less than thirty days, with the statutory period of 60 days in no way being exceeded.



In ten cases, complainants turned to the Office with a complaint against the conclusions reached by the Office's inspectors or against the approach taken by the Office's inspectors when conducting inspections. One complaint was deemed warranted and two partially warranted. In each case, the complainant was informed about the ascertained error and the consequences for the case in question. The remaining seven complaints were found to be unwarranted.

Twenty five complaints pertained to the approach of the Public Affairs Department, which first analysed the complaints and instigations received by the Office. Complaints on the approach taken by the Public Affairs Department usually pertain to the complainants' disagreement with the way their previous complaints were resolved, mainly that the complaints were dismissed without further measures; none of the complaints pertained to inappropriate conduct on the part of Office staff.

In such cases, a review is undertaken of the respective complaints and the approach to handling the previous complaints. Of the complaints received, suspicion of a breach of Act No. 101/2000 Coll. was found in ten, with seven being found warranted and three partially warranted. The remaining fifteen complaints were assessed as unwarranted. If the review of the complaints confirmed suspicion of a breach of Act No. 101/2000 Coll., they were forwarded either to an inspector of the Office for examination or to the Administrative Operations Department to commence administrative proceedings on suspicion of perpetration of an administrative offence or misdemeanour.

It holds in both of the above cases that should a complaint be found warranted or partially warranted, this fact can attest to a system-related error on the part of the Office and can thus be an impulse for further discussion of the issue at hand or for the elaboration of a general standpoint or for the adoption of some other measure by the Office.

As was the case in the previous year, none of the 39 complaints received by the Office concerned the inappropriate conduct of Office staff. Based on this finding, it can be stated that the Office, when handling complaints, communicates with the public on a professional level and in compliance with the principles of protection of the rights and interests of the addressees of public administration.



## **ANNUAL REPORT SUMMARY**

Office for Personal Data Protection

Pplk. Sochora 27, 170 00 Prague 7 E-mail: [posta@uouu.cz](mailto:posta@uouu.cz)

Internet address: [www.uouu.cz](http://www.uouu.cz)

Based on the obligation imposed on it by Article 29(d) and Article 36 of Act No. 101/2000 Coll., on personal data protection, the Office for Personal Data Protection published this annual report on its website in February 2015.