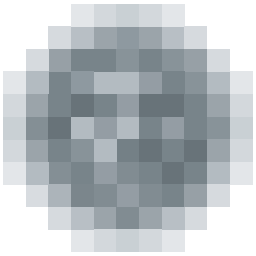
Annual Report Summary 2015



úřad pro ochranu osobních údajů
the office for personal data protection

ISBN 978-80-210-8144-4

Foreword by the Office President

Ladies and gentlemen,

I present to you the Annual Report of the Office for Personal Data Protection for 2015. I was selected as President of the Office by the Senate and then appointed by the President of the Republic effective 1 September 2015, thus I only had the opportunity to influence the direction and activity of the Office for less than half of last year. This report, however, as the law requires, naturally also includes the period before my arrival. As this is my first annual report, the opportunity presents itself to reflect upon the fundamental questions of the purpose, significance and place in society that the Office for Personal Data Protection should occupy in the future.

The Office for Personal Data Protection was set up to protect privacy during the processing of personal data, i.e. information concerning specific individuals. It is no simple matter to define the term "privacy", and there is perhaps no universally accepted definition. In my opinion it can be said that privacy today in our cultural milieu must be seen as part of the personal sphere of every person, comprising both information on their identity, life, place and status in society, and expressions of the personality of a unique human being including their thoughts and opinions and interactions with others. Without privacy, without the possibility of being alone at least somewhere and sometime and deciding what to tell others about oneself and what to keep for oneself, a person cannot be free. And without free people who are also responsible for their lives and their deeds, there can be no free and just society.

I do not think that it is solely the Office for Personal Data Protection that can ensure human privacy and thus the freedom and dignity of the individual. Above all each of us must tend to the protection of their rights. The role of the judiciary is also essential. In order for the Office for Personal Data Protection to fulfil its role, it must be thorough, convincing and coherent, both in oversight and proceedings on breaches of the law, and in formulating and lobbying for its comments on new draft legislation. No less important is its role as an advisory body for the professional and general public. I am convinced that without a strong, independent and efficient Office watching over the processing of personal data in various ways, the protection of privacy would be much more difficult.

Conflicts of interest occur naturally in human society, with various people or groups of people defending different interests. To some extent, privacy and personal data protection are inherently opposed to the right to acquire and disseminate information, just as we can view human privacy as standing opposed to security of the state, which must have as much information at its disposal as possible.

In order to resolve such a conflict of rights, proportional reasoning must be applied in the decision-making process (the proportionality test), with several steps assessing whether the infringement on fundamental rights is necessary, whether it furthers a legitimate objective and also whether it is commensurate.

I am convinced that the goal of those who deal with such clashes in practice, including the Office for Personal Data Protection, should not be to blindly defend only one of those rights and downplay the other regardless of anything else, but to always assess the situation comprehensively, with consideration for all the circumstances and specifics of the given case. Only such an approach can lead to meaningful discussion, rational and fair application of the law and ensurance of a sufficient level of protection for all interests concerned. Hindsight shows that the Office for Personal Data Protection has not always taken this approach, and the outcomes of certain cases have sounded rather one-sided. Thus one of my goals as head of the Office has been and still is for its decisions in all cases to take into account and respect the rights and interests of all entities affected, naturally while also thoroughly yet reasonably protecting human privacy. For these reasons, several of the Office's older positions are being re-evaluated.

In this regard I must also mention the fact that in public debate the Office for Personal Data Protection is often alone in its appeals on the importance of protecting privacy, even though as an oversight body it reacts in most cases to the complaints of entities laying claim to protection of privacy. While other rights or interests have many often very vocal supporters, the importance of privacy as a fundamental value of civilisation tends not to be brought up as frequently in public debate. Another of my objectives is thus for the issue of protection of privacy to be publicly debated, both on a general level and specifically in relation to a certain technology, bill or new register. A first step in this direction is my intention to submit the drafts of new Office positions and similar interpretation documents for public consultation before their approval, but of course I am open to other possibilities on how to bring the topics the Office for Personal Data Protection deals with closer to the public as well.

For the output and opinions of the Office to be of benefit to the public, they must meet several criteria. The first we can call factual accuracy – particularly where the Office is commenting on new technologies it is necessary to understand them and their possibilities, advantages and disadvantages for those who want to utilise them as well as for people whose data are to

be processed by such a new technology. No less important is the legal quality of the Office's output. Aside from a proper interpretation of all relevant regulations, its argumentation must also respect the principles of the rule of law, including related court rulings. Last but not least, the Office's output must be fair and thoroughly substantiated so that, in the diction of the new Civil Code, even a person of average intelligence is able to consider and assess the conclusion. If the general public does not find that the Office's decisions are just or well-reasoned in borderline or controversial cases, the position and reputation of the Office among the general public will not be what it should be relative to its importance.

Aside from the impulses brought by everyday life and practice, the Office also faces a significant change to the legislation. At the level of the European Union, negotiations have ended on a new legal framework, with the existing Data Protection Directive from 1995 to be replaced by a new general regulation that is to enter into force in spring 2018. This change will not only place demands on the oversight body, but also on Czech lawmakers, who will have to adapt the Czech legal code to the new regulation, which is superior to ordinary laws, and especially on entities that process personal data. Preparing the Office for Personal Data Protection and getting involved in the other follow-up activities associated with the new legal framework must be considered one of the top priorities for 2016 and the years beyond.

In light of the above I have moved to reorganise, or rather modernise, the Office so that it is able to better and more efficiently handle the current situation marked by the significant spread of new technologies.

The first major step consisted of fully separating oversight activities by creating an independent Supervision Department, which will have at its disposal experts in special areas of personal data processing and cooperation with foreign oversight authorities. This consolidated supervision will be able to deal with new special tasks and provide specialised support to Office inspectors.

The second major change is the creation and gradual staffing of an analytics unit, the activity of which is to support the supervision conclusions of the Office in administrative proceedings. The analytical activity will monitor and evaluate the current decisions of the Office, particularly in light of the case law of the highest courts in the Czech Republic, as well as with regard to foreign supervisory trends (the decisions of partner bodies for personal data protection in the whole EU) and the case law of the European Court of Human Rights and the Court of Justice of the European Union. With this analysis, a new knowledge base will emerge that will allow the Office to react more quickly and purposefully to changes and new approaches in an area as dynamic as the processing of personal data.

I believe that the Office for Personal Data Protection, even with its position in the complicated system of the Civil Service Act, the tasks and contempencies entailed in protecting personal data, and its organisational and staff base, can and must play an important role for the citizen. This role is not however complete without the cooperation of those who are not indifferent to the fate of their privacy. And that should be all of us!

Ivana Janů
President of the Office for Personal Data Protection

Contents

The Office in numbers 2015

Enquiries and consultations	from the Czech Republic	2901
	from abroad	18
	of those	
	private sector	2134
	public administration	767
Submissions and complaints	total received	1433
	complaints passed along for inspection or administrative proceedings	230
Inspection activities (excluding inspections concerning Act No. 480/2004 Coll.)	commenced	135
	completed	113
	referred to other state authorities	5
	remedial measures imposed	15
	contested by objections	16
	objections upheld	3
	rejected	11
	mostly upheld	1
	mostly rejected	2
	pre-inspection operations without subsequent commencement of inspection	43
Unsolicited commercial communications (jurisdiction under Act No. 480/2004 Coll.)	total complaints	5409
	complaints resolved	4918
	inspections commenced	21
	inspections completed	32
	administrative decisions on a fine	23
	contested by objections	4
	objections upheld	0
	rejected	4
	mostly upheld	1
	mostly rejected	0

	pre-inspection operations without subsequent commencement of inspection	688
Administrative punishment	administrative proceedings for violation of Act No. 101/2000 Coll. and No. 133/2000 Coll.	49
	misdemeanour proceedings pursuant to Act No. 101/2000 Coll.	12
	misdemeanour proceedings for violation of Act No. 159/2006 Coll., on Conflict of Interest	0
	refraining from imposing a fine pursuant to Section 40a of Act No. 101/2000 Coll.	40
	appealed decisions on violation of the law	28
	rejected appeals	19
	overturned and returned for new hearing	3
	decisions overturned and proceedings stopped	4
	change of decision	4
Judicial review (Note: * total since 2001)	court actions lodged	12 (140*)
	actions dismissed by the court	7
	actions overturned by the court	5
	completed/uncompleted court proceedings since 2001	100/40
Registration	notifications received (pursuant to Section 16 of Act No. 101/2000 Coll.)	9389
	processings registered	9037
	still pending	1002
	revoked registrations	106
	notifications of change of processing	787
	proceedings pursuant to Section 17	139
	suspended (no violation of law)	136
	suspended on procedural grounds (e.g. notification withdrawn)	13
	not permitted	4
Authorisation to data to other countries	received requests to transfer personal data to other countries (pursuant to Section 27 of Act No. 101/2000 Coll.)	25
	decisions authorising transfer	21
	decisions authorising transfer	0
	proceedings suspended on procedural grounds	8
Notifications pursuant to Act No. 127/2005 Coll.	notifications received	0
	resolved as justified	0
	resolved as unjustified	0

Complaints pursuant to Section 175 of the Administrative Procedure Code	complaints received	38
	resolved as justified	9
	resolved as partially justified	2
	resolved as unjustified	27

Supervisory activities of the Office

• SUPERVISORY PLAN

In accordance with Section 31 of Act No. 101/2000 Coll., on Personal Data Protection, the supervisory activities of the Office are conducted on the basis of a supervisory plan, or on the basis of submissions and complaints. Preparation of the supervisory plan thus always draws on the objectives of the Office, but some parts of it also directly follow up on the greater interest of society in the Office focusing its supervisory activities in a certain direction, in part as indicated by the number of complaints or submissions signalling a problem in the application of the fundamental tenets of personal data protection in a given area. Another area of inspiration in preparing the supervisory plan are the findings of its employees come to during previous investigations. It is often the case that an investigation that originally focused on a particular matter peels back the veil over a hitherto hidden method of personal data processing and this experience becomes an impulse for the inspector in planning investigations for the next calendar year.

The inspectors themselves take part in preparing and implementing the supervisory plan, and the main reason is that it is they who, in accordance with Section 33 (3) of Act No. 101/2000 Coll., direct inspections and perform other activities within the Office's jurisdiction. Implementation of the supervisory plan is evaluated at mid-year at the meeting of the board of inspectors.

Supervision laid down by the supervisory plan in 2015 focused on several traditional topics, such as **information systems with large amounts of data**. To this end the following entities were inspected:

The Czech Statistical Office, where inspection focused on checking compliance with legal obligations for anonymising data in relation to the census done in 2011; the State Transport Infrastructure Fund; and CzechTourism. Another inspected entity in this area was the Ministry of Industry and Trade and its agenda concerning the authorisation of trade licensing authorities to look into criminal records in connection with proceedings under the Trade Licensing Act.

A separate supervisory activity of the Office was the inspections identified in the supervisory plan as **current cases with greater demands**. An inspection was carried out on an entity operating in the field of postal services. Also in connection with this an inspection was conducted on an entity responsible for processing the personal data of travellers who had filled out and handed in a questionnaire concerning risk areas for preventive measures by the Chief Public Health Officer. The goal of another inspection was to check the processing of personal data by waste producers in connection with the obligations of an operator pursuant to Act No. 185/2001 Coll., on Waste. Other Office inspections in the field of healthcare focused on information systems used in healthcare.

In 2015 an inspection was commenced on compliance with the obligations of a personal data controller in the installation and subsequent operation of preventive devices and elements that help increase the safety and flow of road traffic and monitor it. Monitoring systems were also the subject of an inspection at a targeted water park, where the inspectors focused on checking the camera system for ensuring visitor safety.

Part of the supervisory plan were **inspections based on the international commitments of the Czech Republic**, where the inspectors focused on the Police of the Czech Republic – Foreign Police Directorate in terms of observing the conditions for access and use of data processed under the Visa Information System and on the Ministry of Foreign Affairs in terms of the observing the conditions for access and use of data processed under the Visa Information System.

Aside from the supervisory plan, some supervisory activities by inspectors are carried out at the **orders of the President of the Office**. This concerned an inspection of Prague City Hall, which focused on observance of obligations in administering assets in connection with the leasing thereof, and measures were imposed to remedy the identified findings. This was also the case for an inspection of the Centre for Applied Economics, which is the operator of a portal concerning the financing of political parties. Through this portal the personal data of donors to political parties are published. This was also the route by which the Office repeatedly dealt with the case of the operator of the website www.znamylekar.cz.

• FINDINGS OF INSPECTORS FROM SUPERVISORY ACTIVITY

A. UNSOLICITED COMMERCIAL COMMUNICATIONS

Traffic7 s.r.o.

This was an inspection of the company Traffic7 s.r.o., on which the inspectorate had collected 336 complaints for sending unsolicited commercial communications. The subject stated that the recipients in question are not its customers, but the customers of other entities from whom the subject purchased a licence to a database with the contacts in question, specifically from the companies GoldMail s.r.o. and M&A Solutions, s.r.o.

In light of the stated method of acquiring the contacts in question, the complainants were asked to state whether they had ever provided consent to the sending of commercial communications to the aforementioned companies or if they had ever been registered users of the web portals in question. The complainants unanimously declared that they had never provided consent to the above entities, nor had they registered at their portals.

Section 7 (3) of Act No. 480/2004 Coll., on Certain Information Society Services, introduces the "opt-out" principle as regards commercial communications sent by electronic means to the addresses of customers, or subjects of existing commercial relationships. It is the obligation of the inspected entity to prove that it had prior consent to the sending of commercial communications from the recipient or that the recipient was its customer. While the subject of investigation did attest the databases of e-mail addresses purchased from GoldMail s.r.o. and M&A Solutions s.r.o. and the contracts with these entities in which the consent of the recipients to the sending of third-party commercial communications is declared, the investigator asserted that electronic contact details purchased as part of these databases are not, in light of the manner by which they were obtained, information acquired from one's customer and thus the provisions of Section 7 (3) of Act No. 480/2004 Coll. cannot be applied to them. This is why paragraph 2 of this provision must be taken into account when applying this law and the opinion must be upheld that the owners of the e-mail addresses listed in such a database did not grant any potential acquirer consent to send commercial communications, and thus this database may not be used for such activity. In light of the above facts, the investigator considered it ascertained that the commercial communications in question in the case of the e-mail addresses in question were sent by the investigated entity without prior consent from the recipients. In the case of 57 e-mail addresses, the investigator also proved distribution of commercial communications following prior refusal by the recipients.

Sanctions in the amount of CZK 1 900 000 were imposed against Traffic7 s.r.o. for the above infraction; in setting the amount of the fine, the Office took under advisement the aggravating circumstances of the number of recipients of commercial communications and the fact that the commercial communications were sent to individual recipients repeatedly. Also taken into consideration was the fact that the commercial communications were highly obtrusive for the recipients, with one of the recipients for example having been sent over 40 commercial communications. In some cases several commercial communications a day were sent to a single

e-mail address or the same commercial communication was sent repeatedly over several days. Another aggravating circumstance according to the Office was the fact that the distribution of unsolicited commercial communications took place over a long period of time. The decision has come into force.

eMarketing CZ s.r.o.

In their complaints, the complainants all stated that they had not provided the inspected entity with consent to the sending of commercial communications. No further findings supported the claims of the company under investigation. Thus it committed a breach of Section 7 (2) of Act No. 480/2004 Coll. For this infraction against Act No. 480/2004 Coll, eMarketing CZ s.r.o. was issued a fine of CZK 1 500 000. In determining the amount of the fine in this case, the Office took as a fact increasing the severity of the conduct the fact that the party committed the illegal actions repeatedly and had to be aware (with regard to prior inspection and administrative proceedings) that its actions were illegal. This decision has also come into force.

ABSOLUT-IN s.r.o.

The inspection was commenced on the basis of a submission in which the complainant stated that the above company sent unsolicited commercial communications to 642 work e-mails of his employees. In its statement, the party under investigation stated that it had indeed sent the commercial communications to the work e-mail addresses of the complainant's employees, but that these e-mail addresses came from publicly available sources. In his submission the complainant stated that neither he nor his employees had provided consent to the sending of commercial communications to the company under investigation. The inspected entity did not substantiate such consent, in fact in its statement it actually confirmed the sending of commercial communications to the above addresses without consent. It thus violated Section 7 (2) of Act No. 480/2004 Coll.

For the above infraction the Office inspector issued a fine of CZK 60 000. ABSOLUT-IN s.r.o. however filed a protest against the imposed sanctions and subsequently an appeal. The appellate authority stated that in light of the fact that the company ABSOLUT-IN s.r.o. on the one hand sent commercial communications to over 600 e-mail addresses but on the other hand immediately adopted measures to prevent the distribution of unsolicited commercial communications in the future, the amount of the fine imposed is quite adequate. This decision has entered into force. ABSOLUT-IN s.r.o. was also acquainted with the option of submitting a request to pay the fine in instalments, of which it took advantage.

B. CAMERA SYSTEMS

Zdraví bez limitu CZ, spol. s r. o.

The subject of this incident inspection was compliance with the obligations laid down by Act No. 101/2000 Coll. concerning the processing of personal data when operating a camera system with a recording device.

The inspection found the following:

A total of five cameras are installed at the company's location. One in the entrance hall monitors the area in front of the entrance to the filing area, where biological samples of clients obtained from medical sample-taking are temporarily stored. Other cameras are located on the facade of the building. The cameras at the location were installed at the request of the company's predominantly foreign clients, who were worried about their parked vehicles and their safety.

After three eLybra measuring devices, a laptop and a coffee machine were stolen from the company, its executive filed charges to the Police of the Czech Republic against an unknown perpetrator. Over the course of the investigation, the police authorities stated: "As the company's building is hooked up to a central security console and is equipped with a camera security system, it was evident from the received camera recordings that 3 pieces of lab equipment, a laptop and a coffee machine were taken away." After subsequent investigation the police authorities came to the conclusion that the act did not amount to the crime of theft because it could not be proven that the perpetrator deliberately wanted to seize the items for themselves (it was a former employee of the company) and, in light of the fact that all the items were returned, criminal proceedings were suspended.

The inspected entity issued an Internal Directive No. 1/2015 – Camera System. The camera records are kept for three days in the data storage located in the server room secured by a lockable and coded entrance. Each access to the data is logged and recorded in the operations log stored with the executive of the investigated entity. Records may only be transmitted to criminal authorities and administrative authorities for misdemeanour proceedings.

In connection with the above supervisory findings the following was stated:

The entity under inspection adopted and in Internal Directive No. 1/2015 – Camera System documented measures within the meaning of Section 13 of Act No. 101/2000 Coll. The on-site inspection verified that the recording equipment is truly located in a separate locked room without windows and a coded entrance on the ground floor of the premises. Only the company executive has the keys and numerical code. Access to the records is only possible after entering the controller login and password. No abuse of the camera records took place; they were provided to the Police only in a single case, mentioned above. The technical and organisational measures taken by the investigated party to ensure protection of personal data, prevent access of authorised persons to the means to process them, as well as measures making it possible to identify and verify who the personal data was given to, were found to be sufficient to fulfil the legal obligations arising from the aforementioned provisions of Section 13 of Act No. 101/2000 Coll.

The inspected entity only met the notification obligation pursuant to Section 16 of Act No. 101/2000 Coll. subsequently during the inspection. This fact was evaluated by the inspectors as a violation of the provision in question, but the situation was rectified as soon as violation was identified and the inspector refrained from imposing a fine in accordance with Section 40a of Act No. 101/2000 Coll.

Camera system at Letiny Social and Health Centre

The Office received a complaint from Ombudsman Anna Šabatová against the Social and Health Centre (hereinafter the "Company"), which included an annex entitled "Report on visit to facility", which states that "the installed cameras capture the private life of clients without

any legitimate reason". The report also stated that "there are cameras in the corridors of the whole facility and in the dining halls". The dining hall is where most clients of the individual buildings spend their whole day. Cameras thus record them the whole day and monitor their "private" life without any legitimate reason. The feed is transmitted to the office of the facility's director.

A check showed that the Company had complied with the requirement to register the camera system as per Section 16 of Act No. 101/2000 Coll. In light of the fact that during registration proceedings at the Office concerns arose on the processing of personal data by the camera system in accordance with Act No. 101/2000 Coll., it was imperative for the Company to adopt measures with an "electronic mask" being created on several of the camera shots - part of the view of the common rooms and corridors in the buildings of the centre were covered. On the basis of these measures added to the registration file, the Office suspended proceedings in accordance with Section 17 (2) of Act No. 101/2000 Coll., as it was determined that the party's notified processing does not violate the conditions laid down by Act No. 101/2000 Coll.

The Company installed the camera system in order to protect the rights and interests of clients and employees, to prevent injuries, to ensure quick and effective assistance and to increase the safety and comfort of the provided systems for clients, to oversee the dispensing of medicine, to increase the security of client areas against intrusion by third parties and detect and punish illicit conduct, and to monitor primarily in order to assist and subsequently review causes and adopt corrective measures.

From photo documentation made over the course of the on-site investigation and from camera thumbnails taken during the inspection it was however evident that the limiting of the scope of certain cameras with an electronic mask was insufficient, and despite the modifications made during the registration proceedings client personal data was being processed without their consent in violation of the provisions of Section 5 (2) of Act No. 101/2000 Coll.

In the investigated case these were the areas around the entrances to the rooms where the electronic masks covered only the doors, but not the areas where clients eat or spend their free time. This concerned a total of 14 cameras. In connection with this finding the director of the facility contacted the service company immediately following the on-site investigation and the whole camera system is currently only used in online mode. Thus the objectionable situation was already rectified during the inspection. For this reason the inspector refrained from imposing a fine.

Aquacentrum LETŇANY LAGOON, s.r.o.

The subject of this inspection was the processing of the personal data of visitors collected from the installed camera system with stored recordings via cameras placed primarily in the change rooms of the water park at the headquarters of the investigated party and their publication on the internet.

Before entering the pool area, visitors place their things in lockers and have the key with them for the whole time. In another separate part of the change rooms, separated by a small corridor, are changing stalls separated from the common area so that visitors have privacy while getting changed.

The investigated party primarily operates the camera system in order to prevent damage by carving, drawing, breaking, removal or destruction of the facilities or parts of the facilities, including damaging of relaxation aids so that other visitors can also use them and to prevent

injury on the damaged facilities; the camera system is also operated to protect life and health. The reason for installation of the camera system has proved useful primarily for protecting the investigated party's property and visitors and also for preventing insurance fraud.

Camera recordings led to the solving of crimes by police, with the investigated party's property damaged, customer belongings stolen from lockers, and in several cases camera recordings helped clear up an injury in relation to an insurance claim. Criminal proceedings were launched in several dozen cases since the camera system was installed, with the most recent case being the recording of theft from a locker by camera no. 5, which was the subject of the complaint – the recording from it was published by the Police of the Czech Republic in the media in connection with the search for the perpetrators of this crime.

The recording of the theft of a visitor's wallet from a locker was provided by the investigated party on a flash drive solely to the Police of the Czech Republic in association with this incident. This is demonstrated by the camera system log of 3 January 2015, when the camera recording was given to the police and a written record was made in the logbook on the same day. The recording was published on the internet by the Police of the Czech Republic in connection with the search for the perpetrator who stole the wallet from the locker. The police asked the public for help in finding the thieves caught by the inspected party's camera. The inspected party did not publish the recording of the incident or give it to the media.

On the provisions of Section 5 (1)(e) of Act No. 101/2000 Coll.:

According to this provision, the controller is obliged to only store personal data for the period necessary for the purpose of their processing. The period for which recordings are kept must be set so as not to exceed the period necessary for the incident recording by the camera to be further investigated and other information to be secured, in particular the information needed to pass the case along to the competent authorities for investigation. With regard to the situation at the water park, the period of five days set by the investigated party during which the camera system keeps the recordings made is considered a period necessary for preserving the camera system recordings.

The inspected entity complied with the obligation laid down under Section 5 (1)(e) of Act No. 101/2000 Coll.

On the provisions of Section 11 (1) of Act No. 101/2000 Coll.:

According to Section 11 (1) of Act No. 101/2000 Coll., the controller is obliged to inform the data subject of the scope in which and the purpose for which the personal data is to be processed, who will process the personal data and in what manner, and to whom the personal data may be disclosed, unless the data subject is already aware of this information. The controller must inform the data subject of their right to access their personal data, to correct their personal data, as well as other rights laid down under Section 21. For visitors to the water park this obligation was met via large informational boards, five in number, of which one is installed at the entrance to the water park and four within the complex in visible places. The signs contain detailed information on the area monitored by the camera system, the organisation and safety instructions for operation of the camera system and contact information for the inspected party's executive. The inspected party did not violate the provisions of Section 11 (1) of Act No. 101/2000 Coll.

On the provisions of Section 13 (1) of Act No. 101/2000 Coll.:

In accordance with Section 13 (1) of Act No. 101/2000 Coll., the controller is obliged to adopt such measures so as to prevent unauthorised or accidental access to personal data, the

alteration, destruction or loss thereof, unauthorised transmission, other unauthorised processing, as well as other misuse of personal data. The controller is also obliged to develop and document the technical and organisational measures adopted to ensure personal data protection in accordance with the law and other legal regulations.

Over the course of the inspection the inspector did not find any violations in terms of security breaches of the recording device or other breach of the camera security system. If the Police of the Czech Republic made a recording from the camera system public on the basis of the recording taken from the investigated entity in connection with the search for the perpetrators of theft of personal belongings from a locker of a water park visitor, this was in accordance with the law. The inspected party did not violate the provisions of Section 13 (1) of Act No. 101/2000 Coll.

On the provisions of Section 16 (1) of Act No. 101/2000 Coll.:

The controller of personal data is obliged, before commencing to process personal data of data subjects via a camera system, to notify the Office of this intended processing of personal data. The inspected entity did not submit a notification on the processing of personal data pursuant to Section 16 of Act No. 101/2000 Coll. to the Office, as in its own words it did not know about this obligation. Not only did the investigated entity fail to do so in time, but it did not fulfil the notification obligation even subsequently at the recommendation of the inspector, thus it violated the provisions of Section 16 (1) of Act No. 101/2000 Coll.

The municipality of Ostrožská Nová Ves

The inspector made an inspection based on repeated complaints delivered to the Office in April 2015. The subject of the inspection was compliance in connection with processing the personal data of subjects acquired from a camera system via a camera placed on a pole standing at the edge of a publicly accessible utility road leading to a buffer zone for a Level II water source in front of a "No Entry" traffic sign with an additional sign "except vehicles of SVAK, a.s. and vehicles authorised by SVAK, a.s."

On 3 June 2014 the inspected entity delivered a notification on the processing of personal data to the Office in accordance with Section 16 of Act No. 101/2000 Coll., which it amended 9 July 2014. The Office did not register the investigated party as an controller of personal data obtained from a camera system, as according to the investigated entity's statement, the Police of the Czech Republic was to conduct the processing of the personal data and thus the liberating provisions of Section 18 (1)(b) of Act No. 101/2000 Coll. apply to such processing of personal data carried out under an agenda laid down by a special Act, in this case Act No. 273/2008 Coll., on the Police of the Czech Republic. The inspected party was notified of non-registration of the processing of personal data from a camera system by a letter in July 2014. An inspection was conducted on the investigated party in August to September 2014, which was completed in October 2014. The inspection found that at the time and place of the inspection, the camera system was non-functional, as during trial operation in May 2014 faults occurred in the camera system and, as the cameras did not meet the requirements of the Police of the Czech Republic for image quality, they were disconnected from the recording device until the technical matters could be resolved and the camera system was not further used.

During the course of the subsequent inspection commenced in April 2015 it was found that the camera system was already fully functional and the operator of the camera system as controller of personal data was the Police of the Czech Republic. The investigated party initiated

conclusion of a new coordination agreement with the Police of the Czech Republic. From the perspective of the Police of the Czech Republic the agreement was satisfactory, with the delegation of specific competencies and procedures for processing personal data acquired via the camera system agreed on at several meetings between the party under inspection and the Police so as to avoid infracting upon Act No. 101/2000 Coll.

The result of these meetings was that the controller of personal data from the camera system cannot be the inspected entity, but is the Police of the Czech Republic, even though it is not the owner of the camera system.

Recording from the camera system goes to the hard drive of the inspected party's computer. Only the mayor of the inspected entity has access to the computer if accompanied by a police officer of the Uherský Ostroh District Division of the Police, logging in to the system with his username and password at the request of the Police of the Czech Republic along with the aforementioned police officer and together copying the recording to the police department's external disk. At the Uherský Ostroh District Division the data are backed up for the needs of the Police of the Czech Republic as part of its records under misdemeanour proceedings.

The period for which the recording from the camera system is kept is determined by the Police of the Czech Republic according to its needs. Citizens were already informed about the operating of the camera system, or rather the camera in question, previously (spring 2014) on the municipality's website, in the local magazine *Profil* and through a posting on the official notice board. The information obligation was fulfilled by the inspected party along with the Police of the Czech Republic through information signs with all the required information.

In light of the fact that the inspected entity does not have access to the camera recordings, it could not make them available to another party. The method of use of recordings from the recording device is, in accordance with Act No. 273/2008 Coll., the full responsibility of the controller of personal data, which is the Police of the Czech Republic. In cooperation with the Uherský Ostroh District Division it was ascertained that during the period from 9 October 2014 until 22 April 2015, no recording from the inspected camera system was backed up or used as proof in misdemeanour or criminal proceedings, and the Police of the Czech Republic is awaiting the result of this inspection with the opinion that the recording device could not be used as proof for misdemeanour proceedings for disturbing the peace in Ostrožská Nová Ves if the Office determines it was placed illegally.

According to the provisions of Section 4 (j) of Act No. 101/2000 Coll., a controller is every entity that determines the purpose and means of personal data processing, carries out such processing and is responsible for such processing. The controller may empower or charge a processor to process personal data unless a special Act provides otherwise. The purpose and means of personal data processing in the given case are determined by the operator of the camera system which, based on the Cooperation Agreement on Securing Local Matters of Public Order of 4 June 2009, is the Police of the Czech Republic – Regional Directorate for the Zlín Region, Uherské Hradiště Department, Uherský Ostroh District Division, which may, according to Section 62 (1) of Act No. 273/2008 Coll., if it is necessary for fulfilling its tasks, make sound, image or other recordings of persons or things found in publicly accessible places and sound, image or other recordings of the course of police acts.

According to the provisions of Section 4 (k) of Act No. 101/2000 Coll., a processor is any entity processing personal data on the basis of a special Act or on behalf of a controller. The

investigated entity does not process personal data and thus cannot be a processor of personal data according to Section 4 (k) of the Act on Personal Data Protection either.

The municipality of Ostrožská Nová Ves did not violate Act No. 101/2000 Coll. in protecting its water sources.

C. INDEPENDENT CONTRIBUTIONS

Czech Statistical Office: inspection of anonymisation of data obtained from the 2011 Census

On the basis of the supervisory plan for 2015, the Office carried out an inspection of the Czech Statistical Office ("CSO") focused on compliance and fulfilment of the obligations of a personal data controller in association with the processing of personal data, and checking fulfilment of legal obligations laid down by the special legal treatment, specifically Section 22 (4) of Act No. 296/2009 Coll., on the 2011 Census, i.e. the obligation to have the census forms shredded after the results have been processed, at the latest within three years of the effective time of the census, the obligation to anonymise the census forms converted into electronic form during processing and electronic forms filled out by obligated persons and transfer them to the National Archives for permanent storage.

The census is the most extensive statistical survey and brings in a great amount of valuable data that currently cannot be obtained in any other effective manner. A great amount of personal data is collected and handled in this statistical survey, including data for which the law lays down a stricter regime for protection - sensitive data.

CSO carried out the 2011 Census on the basis of the legal authorisation of Act No. 89/1995 Coll., on State Statistical Service, and Act No. 296/2009 Coll. The collection of data took place using forms.

The inspection found that CSO converted all data acquired into electronic form in accordance with the law, i.e. all paper forms were scanned. The exception were the forms "Residential sheet – continued", which were not converted into electronic (digital) form, were not anonymised and were shredded after processing. These forms contained solely personal data, specifically personal data of persons sharing a household (name, surname, date of birth and relationship to person who filled out the form), and thus were not handed over the National Archives for archiving.

All forms converted into electronic form were then anonymised. This was done by "blacking out" the appropriate boxes into which the respondent had filled in the data on the image of the form. Either the whole field was blacked out (contents rendered unreadable) or part thereof (part of field remains readable).

Once anonymised, the forms were passed along by the legal deadline to the National Archives for permanent archiving. All non-anonymised paper forms and non-anonymised forms converted into digital form were destroyed within the legal deadline (placed into shredding proceedings). The inspected party established clear rules for the whole shredding process. It was found that the collection and destruction of materials was carried out in the required timeline, with no serious incidents taking place during the shredding process and during the whole operation.

The inspection found that CSO adopted measures for the whole process laid down by Act No.

296/2009 that can be considered sufficient to meet the legally stipulated obligations of a controller and processor of personal data.

According to the results of the inspection, the Czech Statistical Office did not violate the provisions of Section 5 (1)(e) or Section 13 of Act No. 101/2000 Coll. and acted in accordance with Section 22 (4) of Act No. 296/2009 Coll. The inspected entity kept the personal data only for the period necessary to fulfil the purpose of processing and anonymised the personal data by the legally stipulated deadline while adopting such measures as to ensure maximum protection of the processed personal data.

The inspection report was delivered to the inspected entity on 3 November 2015. No objections were raised against the inspection report and the inspection was concluded 19 November 2015.

Mezinárodní vězeňské společenství, z.s. (Prison Fellowship)

The inspection was launched on the basis of a complaint from a complainant that asked the Office to assess whether a form distributed by the inspected entity to inmates in prison, which after being filled out contained identifying information on children and caretakers, violates Act No. 101/2000 Coll. The subject of the inspection was compliance with the obligations of a personal data controller in connection with the processing and further handling of personal data in implementing the Angel Tree programme.

The inspection found that the inspected entity has been implementing the international programme Angel Tree, which is a registered programme of Prison Fellowship International, since 2011. The programme is organised with the goal of helping the children of convicted parents. It was found that in some cases other relatives of a child or person close to them (step-father) also registered for the programme. Volunteers involved in the programme send Christmas presents to the children of parents or other relatives serving time in prison. The programme is realised by having a contact person in the prison, generally a social worker or chaplain, approach suitable candidates who are serving time. These identified inmates fill out a form and write a Christmas letter to their child. The prisons then send the filled-out forms along with the letters to the programme coordinator (a representative of the inspected entity), who then organises the purchase and sending of a gift to the child with parishes involved in the programme. The goal of the programme is to strengthen the bond between the child and parent serving prison time for those parents who have not been deprived of their parental responsibilities by court or have not had their right to interact personally with the child restricted.

As part of the Angel Tree programme, the inspected party processes the personal data of the prisoner, the contact person in the prison, the child to receive the gift, and the person taking care of the child (affected person).

The inspection found that the provisions of Section 5 (2), 11 (1) and 16 (1) of Act No. 101/2000 Coll. were violated, i.e. the obligation of the controller to process personal data only with the consent of the data subject, to inform the data subject of the scope in which and the purpose for which the personal data are to be processed, who will process the personal data and in what manner, and to whom the personal data may be disclosed, and the obligation of the controller to notify the Office in writing of its intended processing of data before commencing such processing. At the time of the inspection the inspected entity did not have at its disposal the demonstrable consent of all affected subjects, i.e. of all persons whose personal data are processed on the given form as part of the Angel Tree programme. Even taking into

account the specific nature of the programme, it was found that the inspected entity did not exhaust all options for acquiring consent to processing of personal data of the affected subjects and ensuring that all persons were acquainted with the fact that their personal data are being processed as part of the Angel Tree programme and thus should have the opportunity to express their consent or refusal of the processing of the personal data that can be acquired from the form. It was also found that the inspected party did fulfil its information obligation to the prisoners, the contact persons at the prison, and the children via the one of their legal guardians that filled out the form. The case was different for fulfilment of the information obligation for the processing of personal data of children being sent a gift by someone other than their legal guardian. Here the information obligation could not be met. It was also not possible to verify which caretakers were informed of the project and in what detail. The information obligation could have been met at least for those caretakers who were contacted by telephone and those whom the prisoner had informed. It was also found that the inspected entity had processed personal data in connection with the Angel Tree programme without notifying the Office demonstrably at least since autumn 2011 and only submitted a registration application to the Office on 10 September 2015, i.e. during the inspection.

Violation of other provisions of Act No. 101/2000 Coll. was not found.

Over the course of the inspection the inspected party rectified the unlawful situation immediately after discovering it had violated its obligations, specifically by limiting the programme only to the parents (legal guardians) of the children. It also thoroughly established an obligation for the imprisoned parent to inform the caretaker of processing of their personal data by the inspected entity. It amended the form "Application for Angel Tree Programme".

The inspected party insured that the affected subjects were informed of the fact that their personal data would be processed as part of the Angel Tree programme and that they could withdraw their consent at any time. Through these measures the inspected entity rectified the unlawful state it had caused through its actions during the course of the inspection, i.e. immediately after it was determined that it had violated its obligations. On the basis of the above, the Office inspector refrained from imposing a fine in accordance with Section 40a of Act No. 101/2000 Coll., as the personal data administrator remedied the unlawful state immediately after the breach of duty was detected.

DUKLA Jihlava - mládež, z.s.

The reason for commencing the inspection were repeated complaints from the parents of children who are members of DJ-mládež and are registered with the Czech Ice Hockey Association ("CIHA") that the personal data of their children are being processed without parental consent in a manner different to the one declared by the personal data controller in the registration form, having been passed along without authorisation to other entities, and that they are refused information on how the personal data of their children are being handled.

The inspection found that DJ-mládež was founded 17 February 2000 as a voluntary association of natural persons engaged in physical education, sport, educational and economic activity focused on ice hockey and figure skating. In 1998 the city of Jihlava established HC Dukla, s.r.o. as the successor organisation of HC Dukla Jihlava (a hockey club that had existed since before 1989), which in the past had been funded as a military club and after 1989 was gradually transformed into a limited-liability company 100% owned by the city of Jihlava. Both

entities (HC Dukla Jihlava, s.r.o. and DJ-mládež) register every year in the hockey league organised by CIHA jointly under a single hockey club. The inspected entity concludes a cooperation agreement with HC Dukla Jihlava, s.r.o. ever year, which is required by CIHA so that the two entities can enter the CIHA competition together. It was also determined from the aforementioned contracts that HC Dukla Jihlava, s.r.o. holds the right to the competition, has been leant the registration rights of the inspected body's members and is also the holder of marketing rights.

CIHA's Internal Directive No. 44 governs the rules under which the personal data of players, coaches, referees and other members of hockey clubs are handled. The personal data, including ID numbers, can be provided to the Czech Association of Physical Education and Ministry of Education, Youth and Sport on the basis of consent by the data subjects or their legal representatives in order to keep records on membership levels and for the associated provision of state subsidies.

The inspection showed that DJ-mládež is the controller of the personal data of its members, thus also the personal data of the children of the complainants. The inspection found that the processing of member personal data by the inspected party was entrusted to the company HC Dukla Jihlava, s.r.o., which processes the personal data of the inspected entity's members for the purposes of their participation in the CIHA hockey competition. This was evident from the commercial contract through which HC Dukla Jihlava, s.r.o. committed to ensure the participation of the inspected party's youth teams in all age categories in competitions run by CIHA. Also, in the document "HOK declaration", both entities jointly declare that the registration rights of a player in a CIHA competition are entrusted for a period of one season to HC Dukla Jihlava, s.r.o.

The purpose of the processing of personal data is evident from the registration rules of CIHA, approved at the CIHA conference on 14 June 2014, where it is stated that players who want to take part in ice hockey competitions are obliged to register. The obligation of the personal data controller pursuant to Section 5 (1)(a) of Act No. 101/2000 Coll. to establish the purpose for which personal data are to be processed has thus not been violated. No violation of other obligations arising from Section 5 (1) of the Act in question was found either (collection of personal data beyond the framework of the specified purpose, storage of data beyond the period necessary for the purpose of processing or processing of data for another purpose).

The inspection showed that the inspected entity, as the controller of its members' personal data, has the consent of the data subjects to processing of personal data based on the registration forms for the complainants' children. This is a legitimate legal entitlement to processing personal data within the meaning of Section 5 (2) of Act No. 101/2000 Coll.

The inspection found that the inspected entity only partially fulfilled the information obligation pursuant to Section 11 (1) of Act No. 101/2000 Coll. to the data subjects, or their legal representatives. Above all it did not inform them that their personal data would be provided to HC Dukla Jihlava s.r.o. as well based on the involvement of the inspected party in the hockey club HC Dukla Jihlava registered with CIHA, with both entities (DJ-mládež and HC Dukla Jihlava s.r.o.) performing together under the same hockey club with the registration number 070703. On this matter the inspected entity immediately took measures to remedy the unlawful state found by the inspection by amending the form to include a separate document to be received by the parents or athletes when the application is signed. The inspector acted in accordance with Section 40a of Act No. 101/2000 Coll. and in light of the remediation of the unlawful state during the course of the inspection refrained from a fine.

Visa Information System

In the period from 16 July till 30 November 2015 a follow-up inspection was conducted at the Ministry of Foreign Affairs of the Czech Republic (hereinafter "MFA") based on the Office's supervisory plan for 2015. The subject of the inspection was compliance with the obligations set out in processing the personal data of applicants for "Schengen visas", i.e. 90-day visas, in the Visa Information System ("VIS"). The site of the inspection was the Consulate General of the Czech Republic and the visa centre of multinational company VFS Global in St Petersburg, Russian Federation.

The reason for inclusion of the follow-up inspection in the annual supervisory plan was one of the findings of an inspection of MFA conducted in 2014. The following was stated in the inspection report: "From the perspective of personal data processed in VIS, the use of outsourcing services provided by private companies seems somewhat problematic. 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." In light of the fact that sensitive data on visa applicants is being processed by a private company, the main goal of the on-site inspection was to examine the entire process of handling applications with an emphasis on compliance with all obligations laid down for personal data controllers or processors under Act No. 101/2000 Coll.

The Ministry of Foreign Affairs processes personal and sensitive information on visa applicants, thus it is an controller of personal data. The purpose of processing stems from Council Decision No 2004/512/EC establishing the Visa Information System (VIS). Its functions are laid down by Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the VIS and the exchange of data between Member States on short-stay visas. The goal of VIS is to improve the implementation of a common visa policy, consular cooperation and consultation between central visa authorities – to facilitate the visa application procedure, to prevent the submission of multiple applications to different member states ("visa shopping"), to facilitate the fight against fraud and to facilitate checks at external border crossing points and within the territory of the Member States as well as to assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the EU,

The activity of MFA in issuing Schengen visas is based on the binding EU legislation and especially on Act No. 326/1999 Coll., on the Residence of Foreign Nationals in the Territory of the Czech Republic. The internal procedures of MFA are governed predominantly by internal guidelines that respect the amendment of the Foreign Nationals Act effective 24 June 2014. The issue of protecting personal data is addressed by several articles of the internal regulation on technical and organisational provision for performance of proceedingss and guidelines for processing 90-day visa applications.

The inspection found that the use of the services of VFS Global in the Russian Federation takes place based on a contract signed by Ambassador of the Czech Republic in Moscow Vladimír Remek on 2 June 2014. VFS Global provides the MFA with outsourcing services in

Russia consisting of comprehensive provision of the process for issuing Schengen visas, including taking fingerprints. To this end it currently has 29 visa centres (it operates around 1700 visa centres around the whole world). In St Petersburg, 18 European countries use the services of VFS Global, including countries that are not part of the Schengen area (e.g. Croatia, Bulgaria, Finland). VFS Global provides for the application system for the Consulate General of the Czech Republic, provides comprehensive intake of visa applications including the obligatory fingerprints and provides applicants with other services such as taking photographs.

The private company VFS Global has the status of a processor of personal data within the meaning of Section 4 (k) of Act No. 101/2000 Coll. MFA has met its obligation under Section 6 of the cited Act, i.e. concluding an agreement on personal data processing. Appropriate attention is given therein to the guarantees by the processor related to technical and organisational securing of the protection of the personal data processed in VIS and supervisory activities.

All employees of VFS Global involved in processing personal data when handling visas are continuously trained and regular checks are made of the established procedures. VFS Global has not had to address any security incident involving the abuse of processed personal data in recent times.

The inspection found that VFS Global at its visa centre in St Petersburg and the Consulate General of the Czech Republic have adopted suitable measures in connection with possible risks in the processing of personal and sensitive data of Schengen visa applicants.

Processing of personal data in central registers

In July 2015 an inspection was completed focused on the compliance with obligations by the Czech Republic via the Ministry of the Interior in connection with the access of Czech Radio and Czech Television to information from the central population register. The inspection was conducted on the basis of calls submitted to the Office to investigate the unauthorised access of Czech Radio ("CR") and Czech Television ("CT") to the Population Register of the Czech Republic ("PRCR").

The inspection found that access to the basic registers exists by law on the basis of a request from a public authority. CT and CR have access to the PRCR on the basis of a request from the Ministry of Culture ("MC"). Access to the PRCR for CR was established by the "Decision on Issuing of a Certificate" based on a request for access of a public authority to the services provided. CR utilised access to the PRCR from 24 June 2013 until 9 October 2014. The Ministry of the Interior of the Czech Republic ("MI") dealt with CT's application with a "Decision on Settlement of an Application" and CT utilised access to the PRCR from 9 September 2014 until 9 October 2014.

In a check of administrative proceedings conducted by MI it was then discovered that Act No. 348/2005 Coll., on Radio and Television Fees, is not a legal authorisation for CT and CR to access the PRCR.

Access to the PRCR by CT and CR was terminated with a "Preliminary Measure and Certificate Block" in October 2014 and the MC was called upon to review its "Form for Reporting Proceedings" and draft a new notification for CT and CR with the warning that the jurisdiction of a public authority in an agenda is specified according to the activities and roles, which include the scope of authorisation to various reference items in the PRCR and the scope of authorisations must be stipulated by law.

On the basis of Act No. 111/2009 Coll., the Ministry of the Interior is the controller of the personal data in the PRCR, it performs the processing of personal data of natural persons in the PRCR and is responsible for this processing, thus it is a personal data controller within the meaning of Section 4 (j) of Act No. 101/2000 Coll. and is obliged to fulfil the obligations imposed on data controllers in Chapter II of Act No. 101/2000 Coll., including the obligations under Section 13 thereof to protect that personal data.

On the access of CR and CT to personal data from the PRCR:

Act No. 348/2005 Coll., on Radio and Television Fees, regulates inter alia the subject of the fees, who is a fee payer, the payment of the fees, record-keeping on fees and the exaction of owed fees and surcharges to the fees.

According to Section 8 - Registration of Payers, the administrator of the records on fee payers for radio or television fees is the broadcaster by law. The broadcaster by law keeps records of the fee payers unless it empowers an authorised person to do so, in which case that person is the processor of the fee payer records (par. 1); the fee payer is obliged to notify the broadcaster by law, or the authorised person, that they have become a fee payer (par. 2); in the notification the fee payer must state their name or names, surname, place of permanent residence, for foreign nationals place of long-term residence, and date of birth in the case of natural persons (par. 3). The broadcaster by law, in order to monitor compliance with this law, is entitled to seek out information on unregistered fee payers and keep records in the scope laid down in paragraph 10. According to Section 10 of this same act - Exacting owed fees and surcharges to fees - if a fee payer does not pay the radio and television fee or surcharges to the fees on time even after receiving a request to do so by the broadcaster by law in which an appropriate deadline for payment is set, the broadcaster by law shall be entitled to exact their due in court, including payment of the overdue interest laid down by the civil law regulations.

The Ministry of the Interior argued that it is not entitled to interpret Act No. 348/2005 Coll. It does however have an obligation to assess whether there are legitimate grounds for CR and CT to access the PRCR, i.e. whether such access by CR and CT to the PRCR is established by law, and to what end and what extent.

The cited legislation (Act No. 348/2005 Coll.) does not allow CR and CT access to personal data in the PRCR. The inspection did not find legal grounds for CR and CT to have access to personal data in the PRCR (nor was any claimed during the inspection). This assessment of the situation is also reflected by the measures taken by the MI to terminate the access of CR and CT to the PRCR and the proposed amendment to Act No. 348/2005 Coll. containing legal grounds for CR and CT to access the PRCR. After the inspection was completed administrative proceedings were commenced to impose a fine.

Processing of personal data of students/graduates on the Charles University website

In March 2015 the Office received a submission drawing attention to the suspicion of possible violation of Act No. 101/2000 Coll. in the processing of personal data (personal identification number and place of residence) of university students in the "*Record of the state exam*" and "*Form on course of state rigorous exam*", documents published by the university's Faculty of Social Sciences according to Act No. 111/1998 Coll., on Universities, and stored in the repository of university theses.

According to Section 47b (1) of Act No. 111/1998 Coll., "*Higher education institutions are obliged to make public, at no profit to themselves, the doctoral, Master's, Bachelor's and advanced Master's ("rigorózní") theses that have been defended at their institutions, including the readers' reports and results of the defence. The institution will do this by making available a database of these theses. The means of providing access to these theses is stipulated in the internal regulations of the higher education institution.*"

The method and scope of publishing personal data in the case of the university is determined by the Measure of the Rector, in which the following personal data are listed for publishing: Surname, name, titles, faculty, programme and field of study, type of work, name of workplace that published the work, supervisor, consultant, opponent, supervisor's review, opponent's review, date of defence, report on course of defence and result of defence (classification awarded).

By examining copies made of the state exam records – Bachelor's thesis, state exam records – Master's thesis, forms on the course of the advanced Master's ("rigorous") exams, and records of the course of defence of theses, it was determined that the university faculty has been improperly in fulfilling the provisions of Section 47b of Act No. 111/1998 Coll. for some time now. The university rector immediately adopted measures to remedy the situation.

In light of the fact that unauthorised processing of personal identification numbers and places of birth of students/graduates took place with the publishing of the above documents and violation of Act No. 101/2000 Coll. was demonstrated beyond a doubt, the collected file material for reasonable suspicion of an administrative offence having been committed was passed on to the Office's administrative division for administrative proceedings under Chapter VII of Act No. 101/2000 Coll. For the actions described above a fine of CZK 50 000 was imposed on the university. The decision has come into force.

State Housing Development Fund

Based on a communication sent by the Police of the Czech Republic, in April 2015 an inspection was launched of the State Fund for Housing Development over something that happened in August 2012.

The subject of the inspection was compliance with the obligations connected to the processing of personal data of applicants and beneficiaries of funding provided by the SHDF. The inspection focused primarily on the obligations under Section 13 of Act No. 101/2000 Coll.

The submission concerned the fact that a former employee was said to have "*acquired at an unspecified time in connection with the performance of her job a list of 303 items from a database including the names, ID numbers, telephone numbers and addresses of clients*".

The files sent by the Police of the Czech Republic on a CD contained, inter alia, copies of contracts, amendments and termination of contracts concluded between the inspected party and individual cities around the Czech Republic. The CD also contained around 297 files, with generally two files generated for one client, a Summary of Addresses and a Summary of Contacts containing a name, surname and mobile phone number, plus potentially a personal ID number, permanent residence address and mailing address. All these files were in PDF format and on all of them in the top right corner was: "*Printed by: Name of employee, Loans for Young Families*" and in the lower left corner: "*Date and time printed*".

The Police of the Czech Republic conducted the necessary investigations and took measures to determine the facts indicating that a crime had been committed and the conclusion of the "matter" was that the police authorities failed to prove that the crime of unauthorised handling of personal data under Section 180/2 of Act No. 40/2009 Coll., the Criminal Code, had been committed by a specific person and sent a submission to the Office.

At the Office's request, the SHDF employee suspected of committing a crime stated the circumstances around her access to the personal data that were the subject of inspection, including the fact that she ended her employment at the State Housing Development Fund and signed back all entrusted things, including her keys. She also stated that on the incriminating day, which was a Saturday, she was not and could not have been at her place of employment and did not have an account for remote access to the system.

The Office conducted an on-site inspection at the headquarters of the inspected entity in order to test access to the system. As part of the on-site investigation they attempted to ascertain whether it was possible to access the system (computers) with a universal login and password. This information was not confirmed however. According to the internal regulations the password is changed at regular intervals.

According to the provisions of Section 13 (1) of Act No. 101/2000 Coll., the controller is obliged to adopt measures preventing unauthorised or accidental access to personal data, their alteration, destruction or loss, unauthorised transmission, unauthorised processing, as well as other misuse of personal data.

With regard to the above it is evident that at the time the incident occurred, i.e. in August 2012, the inspected party had not adopted and enacted sufficient measures to prevent unauthorised access to personal data and violated the obligation under Section 13 (1) of Act No. 101/2000 Coll. Since, according to Section 46 (3) of the same Act, the liability of a legal person for an administrative delict becomes extinct if the administrative body has not initiated proceedings within 1 year of the day it learned of it, but not later than within 3 years of the day when the delict was committed, the inspected party was not sanctioned for the found violation.

Activities of sales representatives in connection with negotiating agreements on bundled services

In 2015 a new type of complaint appeared directed against the behaviour of sales representatives in the concluding of contracts for energy supply. The Office conducted two inspections on this issue and also brought administrative proceedings against sales representatives for infractions, i.e. the misuse of personal data without the awareness and consent of the data subjects in whose name the contracts were concluded.

The inspections at companies focused on the "rules of the game" between salespeople and companies, as explicitly set rules determine whether excesses - the misuse of personal data by an employee (sales representatives) - can be attributed to the company or not.

The subject of the first inspection, launched on the basis of a complaint sent in by a Prague municipal district, was compliance with legal obligations by the company BRUNA ENERGY s.r.o. (hereinafter the "Inspected") in connection with fraudulent/unauthorised filling out of contracts by a sales representative that was employed at the Inspected on the basis of an Agreement on Work Performance and who used the personal data of specific persons to conclude agreements on bundled services of electricity and gas supply without their consent and knowledge.

During the inspection the Inspected submitted internal regulations, including an internal regulation entitled Directive on the Handling of Personal Data. The directive laid down the procedures concerning the collection and subsequent processing of personal data by sales representatives. Data are to only be processed to the extent necessary for drawing up and brokering the signature of the contract between the end customer and the provider of natural gas and electricity, and with client consent.

The inspection findings also showed that the Inspected held regular training sessions once a week for its sales partners/representatives focused on the processing of personal data and that the procedures for processing were set in advance for sales representatives: the salesperson was to "contact" the end client through random selection and after mutual consent on the terms they were to fill out the personal data in the columns on a pre-printed form (contract) provided by the supplier, mark it with their ID, leave a copy of the contract with the client and the next morning give the original of the contract to a "back office" employee, who was to copy these data via a password-protected web interface into the supplier's internal system and send the forms in paper for by registered post to the supplier for whom the contracts were concluded.

The evaluation of the inspection focused on fulfilment of the obligations under Sections 13 and 14 of Act No. 101/2000 Coll., as these provisions were crucial for assessing the case.

According to Section 14 of Act No. 101/2000 Coll., employees of the controller or processor and other persons who process personal data on the basis of an agreement with the controller or processor may process personal data only under the conditions and in the scope specified by the controller or the processor. The cited provision means persons involved in the processing of personal data for the controller have an obligation to act solely in accordance with the conditions and instructions laid down by the relevant controller.

The inspection findings showed that the "rules of the game" were explicitly set out by the Inspected, which was a deciding factor for the assessment of the case and determining culpability for the unauthorised processing, as the setting of conditions that employees or other persons coming into contact with personal data at the employer are obliged to uphold is considered one of the fundamental measures under Section 13 (1) of Act No. 101/2000 and then in accordance with Section 14 of Act No. 101/2000 Coll. it is the obligation of employees of the controller to thoroughly heed these conditions and instructions.

These designated "rules of the game" liberated the inspected company from sanctions in the given case and responsibility for the misuse of personal data of (non-)clients was "borne" by the sales representative, with whom administrative proceedings were commenced following conclusion of the inspection and on whom a fine of CZK 2000 was imposed.

The subject of the second inspection was the compliance with legal obligations by the company X Energie s.r.o. (hereinafter also the "Inspected") in connection with the processing of personal data by the distribution company through its business partners. This inspection was also initiated on the basis of complaints delivered to the Office concerning unlawful acquisition and use of personal data to draw up fictitious contracts by sales representatives.

X Energie, s.r.o. submitted internal regulations, including a Directive on Personal Data Protection, the purpose of which was to establish the manner of processing and ensuring protection of the personal data the Inspected uses in its business activities. The directive was binding for all employees and persons in a similar relationship to the Inspected who are involved

in processing personal data. The document laid down confidentiality for all personal data that an employee or person in a similar relationship encounters in their work activity, as well as further measures and principles for protecting personal data. In addition to the aforementioned documents, the Inspected also had an internal document Directive on Technical and Organisational Measures to Protect Personal Data, which describes the method for ensuring protection of personal data.

The investigation findings showed that the Inspected concludes Agreements on Bundled Supply Services with customers using sales groups. During the duration of the contract the Inspected was in contact with the contact person for the sales group, not with individual sales representatives, which it corroborated with the concluded contracts. These contracts obliged sales representatives to perform their activities in accordance with Act No. 101/2000 Coll.

Again in this case the inspection focused on compliance with obligations stemming from Sections 13 and 14 of Act No. 101/2000 Coll.

The findings showed that the Inspected concludes Agreement on Bundled Supply Services with customers using sales groups with which it has an agency agreement signed.

In the agency agreement it is stated, inter alia, that the representative shall operate with due diligence, heed the interests of the distributor and proceed in accordance with its mandate and guidelines. The representative shall also act so as to respect the interests of the customer. The representative furthermore undertakes to perform its activities in accordance with Act No. 101/2000 Coll. and other legal regulations related to the activities performed under the contract. It shall be obliged to acquaint itself with the Sales Code and uphold it. The individual articles of the agency agreement govern the procedures for transmitting the customer contract, amending contracts and verifying communications.

In this case again the inspection findings showed that the "rules of the game" were explicitly laid down by the Inspected in advance, which was the deciding factor for assessing the case and determining culpability for the unauthorised processing. It was evident from the findings that the rules of procedure for the sales representatives were set out in advance and that the individual sales representatives were informed of these rules and committed to them in writing. The misuse of client personal data was thus clearly the responsibility of the persons concluding/signing the contracts. In this case justice was not served however, because even the police did not manage to track down the responsible persons.

These two inspections highlight the fact that the issue of personal data protection is and will continue to be much broader and that it can impact any area of our lives.

Pražské služby, a.s.

An inspection of "collection yards" was included in the Supervisory Plan for 2015 following negative experiences in connection with the identification and registration of natural persons in the purchasing of scrap materials.

The inspection was focused on compliance with the duties of a personal data controller in connection with the identification and registration of natural persons under Section 18 (3) of Act No. 185/2001 Coll. and in light of the fact that the inspection was conducted based on the Supervisory Plan, a whole range of legal obligations were inspected. The findings indicated that the inspected entity meets these obligations and the inspectors did not find, with one exception, any violations thereof.

Though in the given case Section 11 (1) of Act No. 101/2000 Coll. was violated, with i naccurate information being contained in the document intended for collection yard patrons, an interesting aspect of the case is the "legislative imperfection", whereby the explanatory report for the law did not correspond to the wording of the Act.

According to Section 18 (3) of Act No. 185/2001 Coll., the operator of a facility for collecting or purchasing waste conducting collection or purchase of waste identified by the implementing legislation under paragraph 11 shall be obliged to identify the persons from whom it intends to take or purchase the waste, to identify the taken or purchased waste, to keep records of these facts in accordance with paragraphs 4 through 8, including the date and time of taking or purchasing the waste. In order to fulfil this obligation the operator is entitled to demand to see an identification document of such persons; in handling the personal data of natural persons the operator shall act according to special legislation.

The provisions of Section 18 (6) of Act No. 185/2001 Coll. develop the term "identification of persons" and lay out that identification of persons pursuant to paragraph 3 shall mean for the purposes of this Act ascertaining the company name or title of a legal person, the address of its registered office, its company registration number or similar number assigned abroad and the identification of the natural person acting on behalf of this legal entity in the collection or purchase of waste.

It is evident from the paragraphs cited above that Section 18 (6) of Act No. 185/2001 Coll. "forgets" about natural persons within the meaning of Section 23 et seq. of Act No. 89/2012 Coll, the Civil Code. In practice it would otherwise mean the inability of mandatory collection (without consent) of personal data of natural persons not acting on behalf of a legal person, even though waste (e.g. scrap metal) would be collected by the inspected party. The given provision of the act was not quite in keeping with the explanatory report on Act No. 838/2008 Coll., which amended the original wording of the Waste Act. "With regard for the growing price of pig iron, there has been a significant increase in the amount of iron scrap handed in and sold at collecting yards without any subsequent identification of the entity selling the scrap. The reason is the cited provision of the Waste Act does not apply to iron. There is also a lack of the necessary pressure on operators to avoid the purchase of waste that is clearly not waste (e.g. manhole covers, traffic signs, etc.). This led a group of MPs in the fourth term of the Chamber of Deputies to submit a draft amendment to the Waste Act and several other acts that would deal with the given problem."

In assessing the purpose of the law, in particular the lack of a legal basis for processing the personal data of natural persons not acting on behalf of a legal person, the Office also drew on the judgment of the Constitutional Court no. III. ÚS 980/13 of 19 June 2014, in which it states, inter alia: "The Constitutional Court has also declared many times that it does not tolerate the overly formalistic approach used by public authorities, and general courts in particular, using sophisticated rationalisations for a clear injustice. It has emphasised that general courts are not absolutely bound by the literal wording of the law, but that they can and must deviate from this if required by the purpose of the law, the history of its formation, the systematic context or one of the principles that are based in the constitutional legal order as a meaningful whole, and that the obligation of courts to find the law does not mean merely searching out direct and explicit instructions in the legal text, but also the obligation to determine and formulate what the specific law is even where it requires the interpretation of abstract norms and

constitutional principles [cf. judgment Pl. ÚS 21/96 of 4 February 1997 (N 13/7 SbNU 87; 63/1997 Coll.) or judgment Pl. ÚS 19/98 of 3 February 1999 (N 19/13SbNU 131; 38/1999 Coll.)]. In interpreting and applying the legal regulations it is not possible to neglect their purpose and intent, which must not be sought merely in the words and sentences of the given regulation, but must be found also in the principles recognised by democratic legal states [judgment of 16 November 2010 no. II. ÚS 1648/10 (N 226/59 SbNU 299)]."

The inspection also confirmed that large companies, among which Pražské služby, a.s. certainly numbers, do concern themselves with the issue of personal data protection in the course of doing business, and have developed a general methodology and have internal regulations and operating procedures.

In the given case the originally negative experiences with the processing of personal data at collecting yards were not confirmed, which is undoubtedly a good sign in terms of personal data protection.

Plus4U Mobile s.r.o.

The company Plus4U Mobile s.r.o., as a provider of telecommunication services, did not meet the obligation of a personal data controller laid down by the law in that, in offering its services, it acquired new customers through a third party - a broker - but did not have any consent from the new customer to process personal data as it did not have a contract concluded. The company thus processed the personal data of the complainant on the basis of verified personal data acquired without the complainant's knowledge, and at the moment it received these personal data it had sufficient information to know it did not have the consent to process the personal data, nor did it have any legal entitlement arising from the exemptions listed under Section 5 (2) (a - g) of Act No. 101/2000 Coll. In connection with the unauthorised acquisition of the complainant's personal data from the broker, Plus4U Mobile s.r.o. transferred her mobile telephone number from her existing operator to its own account. When the complainant requested things be returned to their original state, the company had her mobile phone number cancelled.

The inspection showed that Plus4U Mobile s.r.o. violated the obligation imposed on it as a personal data controller under Section 5 (1) (c) and Section 5 (2) of Act No. 101/2000 Coll., i.e. the obligation to process only accurate personal data to which it is legally entitled. After the inspection was completed, Plus4U Mobile s.r.o. was ordered to cancel the unauthorised contract and dispose of the complainant's personal data.

CreditPortal, a.s.

The company CreditPortal, a.s. (hereinafter the "Company"), which provides short-term loans, was inspected on the basis of a complaint. This company is dedicated to the provision of short-term financial loans. The impulse for conducting the investigation was the fact that an e-mail was sent from the Company's electronic address containing reminders for three specific debtors. The text of the e-mail contained the name, surname, address, ID number and amount owed. The e-mail correspondence was sent automatically through the Gmail service to more than 88 recipients, all of whom were customers of the Company.

The inspection revealed that the text of the e-mail was generated automatically and its sending also took place based on an automated task. It was stated that the e-mail was sent as a result of an improper intervention into the Company's own software.

The inspection also found that the unauthorised sending took place in connection with a violation of the obligation of a personal data controller under Section 13 (1) (a) and (b) of Act No. 101/2000 Coll., as the Company had not adopted sufficient technical and organisational measures to prevent unauthorised or accidental access to personal data.

The Company submitted objections against the inspection report in accordance with Section 14 (1) of Act No. 255/2012 Coll., the Inspection Code, targeting the finding that the leak of personal data of three clients took place in connection with the failure of the personal data controller to adopt and document the adopted technical and organisational measures to protect personal data.

These objections were rejected.

In the subsequent proceedings the inspector imposed measures to remedy the situation consisting of drawing up current, addressed and factually accurate corrective measures. The Company fulfilled the imposed measures within the deadline.

The Company was enforceably fined CZK 30 000.

Inspection of compliance with obligations of personal data controllers with a focus on consent of data subjects when concluding an agreement based on general commercial terms and conditions

The inspection focused on corporations whose activities is regulated by special legislation. Three entities were inspected: ČEZ Prodej, s.r.o., O2 Czech Republic a.s. and Pražská plynárenská, a.s.

The inspection of ČEZ Prodej, s.r.o. and O2 Czech Republic a.s. was started in 2014 and was completed in 2015. For Pražská plynárenská, a.s., the inspection had not been completed by the end of 2015.

The common denominator of all the shortcomings found in terms of compliance with Act No. 101/2000 Coll. is confusing and ambiguous formulations in informing data subjects about their rights and obligations when concluding contracts and granting (or not granting) consent to processing of personal data for the purposes where the law requires it, and not requiring client consent in cases where the company has the right by law to process personal data without consent.

With regard to the findings from supervisory practice, where the use of business terms and conditions to meet the obligations of Act No. 101/2000 Coll. is in many cases associated with insufficient or incorrect fulfilment of the legal requirements, the Office considered it appropriate to make a statement on the issue of fulfilling the information obligation when processing personal data in business terms and conditions or similar documents. It did so by issuing a methodological recommendation entitled Methodology for Fulfilling Information Obligations and Related Arrangements with Customers, which is available on the Office's website in the section entitled Opinions of the Office.

In general it is the case that, based on the will of two parties –- business and customer – a legal relationship is formed, a contract. The mutual exchange of information is crucial for the emergence and performance of the given legal relationship. The information that the customer provides to the business while negotiating or realising the legal relationship, or which the business acquires from other sources, often includes personal information, i.e. information related to a specific natural person - the customer. The collection and use of this information comprises processing of personal data within the meaning of Act No. 101/2000 Coll., with the business in the position of controller and the customer in the position of data subject, with all the consequences for both sides arising from Act No. 101/2000 Coll.

One of the basic obligations of a controller is to process personal data in an open manner and provide the data subject with a corresponding amount of information about the processing of their personal data. Due to the complexity and interdependence of the various parts of Act No. 101/2000 Coll., in practice there can be problems in interpretation when fulfilling the information obligation, particularly when doing so as part of a document also containing other legal provisions - in business terms and conditions. The best way to thoroughly and properly fulfil the information obligation in a manner that is accessible to the customer would seem to be placing all provisions on personal data processing in a separate document which is referred to in the contract (as is done, for example, with price lists or terms of sale). Such a document should contain all relevant information on the personal data processing which is to take place or which could take place within this relationship. Should the controller (business) decide to include the provisions on personal data processing directly in the business terms and conditions, it is important to at least list all information on this issue in one place within the terms and conditions so that the data subject (customer) not have to search in multiple places or in various documents when seeking the details on personal data processing.

In practice it is no exception that there is superfluous extracting of consent where the law does not require the customer's consent, which in essence is also improper fulfilment of the information obligation and thus a violation of Act No. 101/2000 Coll. as such. In other words, if the controller demands from a data subject consent to processing of personal data required to fulfil the concluded agreement, such an approach is superfluous for both parties and confusing for the customer.

If the processing of data for one of the declared purposes truly must be done on the basis of consent from the party concerned, attention must be paid to the formalities of consent to personal data processing. According to the law, consent is a free and conscious legal act. Should either of these requirements not be met, i.e. it is not free, for example conclusion of the contract is conditioned on the customer's consent to data processing that is not strictly necessary (e.g. for marketing purposes), or if the data subject is not provided with relevant information on data processing before expressing consent, this will be faulty legal conduct. Consent that is not a free or conscious (informed) act is not a valid legal entitlement to process personal data, and if the controller cannot corroborate that it can perform the given processing on the basis of a different legal entitlement, such processing shall be unlawful as a whole.

If the customer believes they have incurred material or non-material damages as a result of unlawful processing of personal data, they shall have to assert such claims in civil proceedings.

Ministry of Education, Youth and Sport

An Office inspector conducted an inspection of the Ministry of Education, Youth and Sport ("MEYS"). The inspection was conducted on the basis of the Office's Supervisory Plan for 2014. The subject of the inspection was compliance with obligations in connection with the processing of personal data in the documentation agenda of subsidy programmes realised by MEYS announced as State Support for Sport for 2013 and 2014. Over the course of the inspection, the subject of the inspection was expanded to include personal data processing in the documentation agenda of the subsidy programme realised by MEYS announced as State Support for Sport for 2015. The inspection was included in the Office's Supervisory Plan for 2014 based on

findings from a previous inspection in which the collection of significant amounts of personal data was shown in order to submit subsidy applications in the field of support to MEYS.

Over the course of the inspection it was determined that, under its subsidy programmes, MEYS requires applying entities (associations) to submit evidence of their member base on a CD-ROM, with the Excel spreadsheets sent on the CD-ROM also containing information on the members of individual associations including: surname, name, date and year of birth, sex, sports club, address, amount of membership fee, e-mail address. MEYS established the purpose and means of processing the personal data, with the purpose of collecting personal data being the transparent funding of sport. MEYS established the criteria and conditions for submitting an application for State Support of Sport, which is formulated in the Guideline for Providing Subsidies Announced under State Support for Sport. Up until 2012 MEYS required only the total number of members from applicants, but since 2013 (or rather, applications for the year 2013) and fully since 2014, it has required from associations a list of members including their personal data in the scope listed above in order to verify that the subsidy is used properly, effectively and economically. This data is given to MEYS in electronic form. MEYS is thus a controller of the personal data of association members, which is processed under the State Support for Sport programme declared by MEYS within the meaning of Section 4 (j) of Act No. 101/2000 Coll.

According to the statement of MEYS, no check of duplicates or triplicates in the applications, i.e. amended member lists, takes place, as it responded to the question, "What is the approach of MEYS in finding duplicated personal data under one or more applicants (e.g. in the relationship between a sports team and the sports association or in the relationship between two independent sports teams)?" by stating that the member lists are not always submitted in such a format (data filled in incorrectly) to allow for the detection of duplicates and triplicates. To the question of whether MEYS conducts a subsequent check that the conditions have been met by checking the member base of an association, MEYS stated that no check is made due to a shortage of staff at the MEYS Sports Department.

On the scope of the personal data processed under the subsidy programme State Support for Sport, the inspectors state that, through the required lists of personal data on members of the associations applying for State financial aid (subsidy), MEYS is collecting member lists including personal data in the scope: surname, name, date and year of birth, sex, sports club, address, amount of membership fee, e-mail address in order to verify that the subsidy is used properly, effectively and economically; the processing of personal data in such scope is not necessary. In order to fulfil the stated purpose, it would be sufficient to process personal data in the scope: name, surname, amount of membership fee, and for a potential subsequent check of the member base by contacting a member to verify whether they are a member of the given entity (see above information on subsequent check of member base), also one method of contact.

It follows from the statements of MEYS and its response to the Office that in essence MEYS is not in conflict with the preliminary conclusions of the Office from the inspection performed, with the main difference being in the understanding of the definition of personal data, which MEYS applies to the personal identification number and the processing thereof, which MEYS does not do. From the text of its statement it is the opinion of the inspectors that to fulfil the established purpose, also taking into account the conclusions of supervisory bodies (Supreme Audit Office and Ministry of Finance) that "the measurable criterion is basic information on

the member base of the association broken down into active athletes, coaches, referees, youth and others", an indication of the total number of members of the applicant (association) with a breakdown by athletes, coaches, referees, youth and others is sufficient.

To check the data on the number of members, including the internal breakdown, other means can certainly be used without having to collect and process personal data to the extent that MEYS has established and implements. MEYS has sufficient powers to conduct checks of the submitted applications, for example by checking the member base evidence directly at clubs, or comparing accounting records on collected membership fees.

By collecting member personal data through the required lists of association members without using them for the state purpose, MEYS as a personal data controller has, according to the inspector, violated Section 5 (1)(d) of Act No. 101/2000 Coll., as under the State Support for Support programme in 2013, 2014 and 2015 it collected the personal data of a great number of entities that does not correspond to the specified purpose and the extent necessary to accomplish the specified purpose.

In the following administrative proceedings, MEYS was ordered to take measures to remedy the shortcomings identified within the meaning of Section 40 of Act No. 101/2000 Coll., specifically to set up control mechanisms under the State Support for Sport programme (General Sports Activities programme) so as not to demand the collection of superfluous personal data on members of sports associations and other entities through which applications are submitted to the proceedings subject to meet the stated purpose when processing state subsidy requests, with the processing of the following personal data being sufficient to meet the stated purpose: name, surname, amount of membership fee, and for possible subsequent checks of member base by contacting a member to verify they are a member of the given entity, one method of contact. The date for the remedial measure to be met was set at 60 days from the order taking effect. MEYS subsequently informed the Office that the imposed measure for remedy had been implemented.

Lázně Darkov

An Office inspector conducted an inspection of the company Lázně Darkov, a.s. (hereinafter just the "Company"), the subject of which was observance of the obligations of a personal data controller, with particular focus on the security of personal information in terms of medical records ("MR").

The inspection of the Company was conducted on the basis of a complaint forwarded to the Office by the Karviná–Mizerov District Division of the Police of the Czech Republic on 22 September 2014, which contained the suspicion that the Company had violated the provisions of Section 13 of Act No. 101/2000 Coll., as it had discovered that the Company had lost the complete medical records of 22 clients/patients. The Police of the Czech Republic sent the Office its case file containing a description of the facts gathered by its own investigation into the matter.

Medical records are a set of information concerning the specific patient about whom it is kept, and which records pursuant to Section 53 (2)(a) and (g) of the above Act identifying data about the patient, including the name or names, surname, date of birth, personal ID number if assigned, public health insurance number and other data including information on the patient's health, the course and results of healthcare services provided and other important

circumstances related to the patient's health and the healthcare services provided, including data from the patient's family, personal or work history and, if justified, data from their social history and other data according to Act No. 372/2011 Coll. or other legal regulations governing healthcare services or the provision of medical care. There is thus no doubt that the Company processes information based on which a specific individual can be identified and information concerning this specific individual, thus it processes personal data according to Section 4 (a) of Act No. 101/2000 Coll. As a provider of healthcare, social, medical, spa and other services, it processes information concerning the health of its clients/patients to the extent governed by Section 53 et seq. of Act No. 372/2011 Coll., thus it handles sensitive data on the patients according to Section 4 (b) of Act No. 101/2000 Coll.

The Office inspector stated that at the latest from 15 July until 1 August 2014 the Company had lost track of the medical records of 22 clients/patients, who had completed their rehabilitative treatment at the spa by 15 July 2014 at the latest. The Company, as a personal data controller, is responsible under Section 13 (1) of Act No. 101/2000 for the loss of 22 sets of medical records with the personal and sensitive data of 22 data subjects containing a medical report on the result of treatment, medication sheet, nursing documentation, spa proposal, informed consent for medical acts, medical history and other documents based on the client's health and the requirements of the attending physician (record of ergotherapy, logopedic report, targeted functional tests and examinations, consultation examinations, descriptions of imaging, ECG record, blood glucose monitoring, monitoring of fluid balance, lab results, approval of stay guide, approval of prolonging of stay by health insurance company, reporting of hospital and other infections, request for access to and procurement of medical documentation, report on client fall, health and social record, treatment document). The Company thus as a personal data controller violated the obligation of a controller under Section 13 (1) of Act No. 101/2000 Coll., as it failed to adopt such measures as to prevent the loss of personal and sensitive data collected in the medical records of 22 data subjects.

In reaction to the sent Inspection Report, the Company sent the Office information on the expansion of technical and organisational measures adopted at all levels of provision of healthcare services where medical personnel come into contact with MR. The Company introduced demonstrable transmission of the MR or part thereof from admission of the patient/client, through the course of their treatment to the depositing of the MR in the Medical Record Registry. The quality management system of the Company was expanded to include internal audits focused on observance of the regulations concerning handling of MR. Repeated checks were done on the authorisation of healthcare workers to access the electronic MR system, records of keys and lending of medical records from the Medical Record Registry, with such lending restricted to the director of medical care and the head nurse with demonstrable records made of the process.

With regard to the above information on the expansion of technical and organisational measures the Office did not launch administrative proceedings on remedial measures with the Company as it considered the measures adopted sufficient.

In the subsequent administrative proceedings the Company was issued a fine of CZK 220 000.

Mnichovo Hradiště and operation of transparent bank accounts

The reason for the launching of the inspection was a complaint the Office received from a complainant that the city of Mnichovo Hradiště (hereinafter the "City") was using a transparent bank account starting 1 May 2015 for incoming payments, including certain administrative fees (fines, waste fees, etc.). In the summary of payments was then information about the payers, such as: name, surname, bank account number, amount paid, purpose of payment and sometimes even their address. The complainant also stated that he thinks that some payers have no idea that such information is being published in this way. He is also of the opinion that this violates Act No. 101/2000 Coll.

Over the course of the inspection it was found that the City set up seven transparent accounts of a total of 14 accounts as part of a transparent approach to asset management starting 1 May 2015 on the basis of a contract or contract addendum with Komerční banka, a.s. After consulting with representatives of the municipalities that already operate transparent accounts and on the basis of a decision of the City Council of 3 August 2015, the City reduced the number of transparent accounts to three.

The City informed its citizens on the establishing of the transparent accounts and possibilities for payment on the City website by publishing the relevant City Council Resolution on the City website, by publishing the information in the *Boleslavský deník* newspapers and by publishing it in its own municipal newsletter.

Citizens can make payments through the appropriate transparent account or in cash or by payment card at the cash desk of the Municipal Authority. For contracts concluded with natural persons after 1 May 2015, the City provided information (by written notification) about the fact that payment is to go through the transparent account. The City then concluded an Addendum to the Account Agreement between Komerční banka, a.s. and the City of 29 April 2015 for seven accounts – the client and bank agreed that the Transparent Account service would be provided for the accounts, under which the bank would publish on its website (www.kb.cz) the account number, client identification data and the following information on the payment transactions recorded to the account: amount and currency of transaction; date payment is record to account; description of payment; account name of payer if transmitted by sending bank; message for recipient; variable, constant and specific symbol if included by payer. The addendum also contains a clause that the client hereby grants the bank consent to publish the information under the previous article and the client undertakes to inform the payer in an appropriate manner that the information on payment to the account will be published in the above scope and above manner. Under the Transparent Account service, information on all payment transactions credited to the account for the last 180 days will be displayed.

Based on the findings it can be stated that along with identification of the payment, on the basis of the above information it is also possible to identify the payer, i.e. a specific natural person. Through the transparent account, data is processed that is personal data within the meaning of Section 4 (a) of Act No. 101/2000 Coll. The City set up transparent accounts on the basis of an addendum to an agreement concluded with Komerční banka, a.s. in order to inform citizens on the financial management of city representatives, thereby also deciding that information on payments (including personal data) would be publicly accessible. The City is thus a controller of the personal data of citizens (payers) whose data is published through the City's transparent accounts within the meaning of Section 4 (j) of Act No. 101/2000 Coll.

The Office inspector stated that citizens of the City were demonstrably informed about the nature of the transparent account but were not informed sufficiently on what specific information in connection with the payment made would be published in the transparent account as stated in the Addendum to the Account Agreement between Komerční banka, a.s. and the City. In setting up the transparent accounts the City did not sufficiently inform specific payers about the possibility of making payments not just by bank transfer but also by other means, e.g. in cash or by payment card at the City cash desk.

Over the course of the inspection the City proposed filling in the information obligation within the meaning of Section 11 (1) of Act No. 101/2000 Coll. by ensuring general information (text) on the City's website, official notice board and the city newsletter in December 2015.

In the inspection report the Office inspector stated that in introducing the Transparent Account service the City did not provide citizens with clear and sufficient information on the processing of their personal data through publishing in relation to payments through the City's transparent accounts, but over the course of the inspection the City prepared an expansion of the information on payments through City transparent accounts and promised to fully implement this by the end of 2015, so the Office inspector stated that the City was not in violation of Section 11 (1) of Act No. 101/2000 Coll.

Other supervisory activities

• COMPLAINTS HANDLING AND CONSULTATIONS AGENDA

In 2015, as in previous years, the Public Relations Department provided for initial performance of the complaints handling within the meaning of Section 29 (1)(c) of Act No. 101/2000 Coll. and the vast majority of the consultation agenda of the Office pursuant to Section 29 (1)(h) of the same Act.

In terms of the complaints handling, the Public Relations Department assesses dozens of received complaints and suggestions, conducts analyses thereof and on the basis of the results handles them appropriately. Most frequently it informed the complainant that it found no reasonable suspicion of violation of Act No. 101/2000 Coll., and recommended what steps to take; some submissions it passed along to the appropriate authority. In justified cases where the submissions gave rise to suspicion of violation of Act No. 101/2000 Coll., these submissions were passed on for inspection or administrative proceedings. In 2015 over 200 individual submissions were passed along in this manner, being further dealt with by other Office units. It is necessary to emphasise that in all cases the complainants were communicated with within the legal deadlines and each complainant was sent information on the assessment of their submission, even in the case that the submission was not found to justify an inspection or administrative proceedings, in which case the reasons for this were explained to the complainant and often further steps were recommended, e.g. taking advantage of the rights under Section 12 and 21 of Act No. 101/2000 Coll. with the option of contacting the Office again if the explanation provided by the controller is not satisfactory or they consider it in conflict with the Act or no explanation is received. This approach seems to be effective in part because the data subject thus "exhausts" the active options to protect their personal data afforded by Act No. 101/2000 Coll., and with the submission of further information from the complainant, for example the controller's response to their request, the Office receives further information and materials for potential subsequent steps in the form of an inspection or administrative proceedings.

Consultation activity consisted primarily in answering written questions, primarily sent electronically, as well as providing telephone and personal consultations. It can be stated that the topics of complaints and consultation are the same.

The dominant topic was, traditionally, camera systems. A new phenomenon is electronic peepholes on residential doors that make recordings.

A number of questions and complaints also focused on the issue of the legitimacy of the process of various entities when making copies of personal and other documents.

A considerable number of complaints also concerned various debt registers, and as part of consultation activity the differences were explained between a bank register kept on the basis of Act No. 21/1992 Coll., on Banks, and non-bank registers without a direct basis in the law.

Complaints and questions also concerned the traditional topic of handling of one's personal identification number and the use of ID numbers in light of the fact that, although the ID number is not sensitive data within the meaning of Section 4 (b) of Act No. 101/2000 Coll., it does enjoy special legal protection via the fact that its use is governed by special legislation.

The ambiguities that were to be removed by the amendment to Act No. 128/2000 Coll., on Municipalities, persisted in opinions on the possibility of a municipality to congratulate its citizens on important life events. Questions on the making of audiovisual and text records of municipal assembly meetings were also frequent, and it was explained that the main criterion for being able to make such records public is whether the issues discussed are public or are problems concerning the private life of citizens, in particular social or health issues, the publication of which, particularly on the internet, would be an unjustified invasion of privacy.

Often it was necessary to straighten out the opinions of enquirers on the possibility of withdrawing consent to personal data processing caused by improper information provided by a personal data controller and acquisition of consent in cases where it is misleading, e.g. to conclude a contract, which can of course not be confused with forcing consent for other purposes. Such misleading information is provided even by large entities where one could expect that they would be able to properly distinguish cases where personal data can be processed without consent and not demand consent in such cases, i.e. that they would only demand consent in justified cases.

Every day a number of telephone enquiries were answered, though in the case of complicated questions it was not always easy to immediately provide an exact and exhaustive answer. More complex consultations concerning what were often new projects associated with personal data processing or for large entities were generally provided with two or more employees of the Public Relations Department present or in cooperation with other Office units. In 2015 the Public Relations Department thus held consultations with entities such as ŠKODA AUTO a.s., Lidl Česká republika v.o.s. or the Sdružení agentur pro výzkum trhu a veřejného mínění [Association of Market Research and Public Opinion Agencies].

• FINDINGS OBTAINED IN ADMINISTRATIVE PROCEEDINGS

At the outset of this chapter it is necessary to note that the results of some administrative proceedings following up on already executed inspections are contained in the chapter Supervisory Activities of the Office. In 2015 the Office conducted over 60 proceedings on suspected violation of Act No. 101/2000 Coll. or Act No. 133/2000 Coll. on the Population Register, and put another 40 matters aside pursuant to Section 40a of Act No. 101/2000 Coll., according to which if the unlawful state is remedied in accordance with the measures imposed or immediately after the breach of duty was detected, the Office may refrain from a fine. The focus of this chapter is to explain several issues associated with the conducting of administrative proceedings encountered by the Administrative Department, which conducts the vast majority of administrative proceedings for offences under Act No. 101/2000 Coll. and other legislation.

One of the issues dealt with repeatedly is the status of individual entities that the proceedings conducted affect in some way. In essence there are three groups:

The first group is made up of those who send the Office the complaint based on which the proceedings are then conducted. Here it should be stated that proceedings on an administrative offence are initiated ex officio, and in no way are these proceedings launched at someone's behest. Related to this is the status of the author of the complaint who, on the basis of Section 29 (1)(c) of Act No. 101/2000 Coll., has the right to be informed on how their submission was dealt with. In keeping with the standard procedure of administrative courts, however, such an entity is not a party to the proceedings on an administrative offence, though this does not preclude, for example, that they could be heard as a witness.

The second group consists of those whose personal data are or were to be processed in conflict with the law, but who did not contact the Office (for various reasons), yet the Office found out about such processing from other sources. Such a reason could be fear of countermeasures, e.g. if the "suspicious" processing is being conducted by their employer. Essentially the same conclusions apply for this category of persons as for the first group: such entities are also not parties to the proceedings but may also be, for example, called as witnesses. Such persons must make any claims against the responsible parties via the courts (see Section 21 (3) and Section 25 of Act No. 101/2000 Coll.).

The third group are parties to the proceedings, i.e. persons who are suspected of committing an administrative offence and with whom administrative proceedings have been launched. These persons have all the rights granted to parties to proceedings by the Administrative Procedure Code (and other legislation), including the option of lodging appeals, etc.

Another question dealt with repeatedly is whether the complainant or author of a submission (i.e. the first group of persons listed above) has the "right" for sanction proceedings to be launched on the basis of their submission in the case of suspicion of violation of the law. It must be stated that no legal regulation sets down such a right. According to Section 42 of Act No. 500/2004 Coll., the Administrative Procedure Code, an administrative body is obliged to receive submissions to launch proceedings ex officio. If the one who made the submission so requests, the administrative authority shall be obliged to inform the complainant within

30 days of the day it received the submission that it has commenced proceedings or that it did not find the grounds to commence proceedings ex officio, or that it passed the complaint along to the competent administrative authority. From this provision the author clearly has solely the right to information, which is undoubtedly a right that also follows from the basic principles of administrative proceedings and, in the case of the Office's activities, also from the already mentioned Section 29 (1)(c) of Act No. 101/2000 Coll., according to which the Office accepts submissions and complaints concerning breach of obligations provided by law in personal data processing and informs of their settlement.

In its activities the Office has repeatedly referred to judgment of the Constitutional Court I. ÚS 4/04 of 23 March 2004, according to which "criminal law and criminal qualification of a certain act that has a basis in private law as a crime must be considered ultima ratio, i.e. an extreme legal means that has a society-wide impact, i.e. in terms of protecting the basic values of society. In principle however it may not serve as a means to replace the protection of rights and legal interests of an individual in civil relationships, where it is primarily up to the individual activity of the individual to protect their rights, for which judicial power provides protection. It is however unacceptable for this protection to be actively taken on by criminal authorities, the primary task of which is to protect societal values, not specific subjective rights of an individual, which by their nature belong in the civil sphere". The above analogously applies in relation to punishment for administrative offences as well, where an administrative offence with a lower degree of societal harm compared to a criminal act is punished, with such punishment also fulfilling a subsidiary role in the legal code. The Office has thus repeatedly come to the conclusion that the application of civil protection is appropriate here, which takes precedence over administrative punishment. The passivity of an individual in protecting their rights, or the insufficient effectiveness of legal instruments serving to protect the subjective rights of individuals, cannot lead to these measures be replaced or supplemented by means of criminal law, or administrative law as the case may be.

• FINDINGS FROM JUDICIAL REVIEWS

As in previous years, in 2015 a good number of Office decisions were subject to judicial review. Only a few judgments were issued in 2015, however, and thus many decisions of the Office are still awaiting judicial review. In terms of specific findings from the judicial practice in 2015, we can point out the following judgments, concerning primarily internet discussions, the publishing of personal data in television broadcasts, the operation of camera systems and several procedural matters:

1. If a certain entity organises an internet discussion on its website, it must invest the effort and resources to cultivate the chat and continually remove expressions that could affect the reputation of third parties. In no case can this responsibility be avoided by saying that the author is not the organiser and contributors cannot be restricted in any way because the "internet is free".

The service provider is not obliged to monitor content of transmitted or saved information, nor to actively seek out facts and circumstances demonstrating the unlawful content of information and is thus not liable for the content of information inserted by users. This ceases to apply however from the moment that the service provider learns of the unlawful nature of the content of such information. Recognised as such a moment was the receipt of a letter from the Police of the Czech Republic asking for information on the poster of a specified post due to an investigation pursuant to Section 158 (1) of Act No. 141/1961 Coll., the Criminal Code. Such a communication may not be left unnoticed and the service provider should address the post on the basis of such.

2. If a legally stipulated prohibition on the publishing of information has been breached, the way in which the given programme or recording was perceived by specific viewers shall not be a deciding factor from the perspective of whether an administrative offence has been committed.

The Municipal Court in Prague stated that an administrative offence under Section 45a (1) of Act No. 101/2000 Coll. was committed by the mere publishing of information making it possible for the identification of damaged parties to be determined. This publishing came to pass as part of the television broadcast of a programme that included a shot of the text of a court ruling containing the legible names and dates of birth of underage children, as well as the names, surnames, dates of birth and addresses of their parents. It is then irrelevant how this report was viewed by the audience.

In connection with this the objection that the data in question could only be determined if one paused the programme on the internet did not stand up.

3. The opinion that it is possible to operate camera systems without the consent of the data subjects, but only if it is absolutely guaranteed that the personal data from that camera system will not be published or otherwise distributed, cannot be generalised and the question of prior consent of the subject to publishing must be assessed with regard to the situation under which publishing of the photograph took place and whose rights could be affected.

In the opinion of Municipal Court in Prague, it follows from the conclusion of the Office that it is placing the protection of the privacy of a criminal offender above the right of an owner to protect their own property. The photograph was made from the course of a crime being committed and moreover the publishing of the photograph on a social network led to the perpetrator being identified. The court thus held that the perpetrator of a crime who deliberately steals property they do not own must count on the fact that their right to respect of personal identity will not be protected to the same extent as the rights of persons acting in accordance with the law. It thus sees no reason why protection should be afforded to those who commit crimes and a person who was merely attempting to ensure the return of their own property of relatively great value by publishing the perpetrator's photograph on Facebook should be fined.

The court also took into account the fact that on news programmes television stations broadcast CCTV footage on which people caught committing a crime appear. In some cases this footage is provided by the police, but not always, which should be apparent from the content of the specific programmes. Allegedly this conduct is often not punished by the Office. In part due to this practice, which however the court did not corroborate in any way, the court became convinced that there is no reason why the publishing of a photograph on a different information portal should lead to a fine.

In this context it is necessary to add that the Office has challenged this judgment with an appeal.

4. If an audiovisual recording made from the website of the single party to the proceedings is made as evidence, it is not a procedural error if the party is not informed of this taking of evidence outside the hearing.

5. For the elements of an administrative offence to have been fulfilled according to Section 45 (1)(c) of Act No. 101/2000 Coll. in connection with Section 5 (1)(f) of Act No. 101/2000 Coll., it is also necessary to demonstrate unlawful conduct from the perspective of the purpose for which the data was collected, which essentially means to ascertain for certain the purpose for which and on the basis of what obligation the collection and processing of personal data is taking place. Likewise, for an administrative offence to have been committed under Section 45 (1)(d) of Act No. 101/2000 Coll. in connection with Section 5 (1)(e) of Act No. 101/2 0 0 0 Coll., it is necessary to demonstrate the period necessary for the purpose of processing, as only after the end of a period for which data can be retained for further purposes (statistic, academic, archiving) does the law demand protection against encroachment on private life for these purposes, which means anonymising the data.

• REGISTRATION

In 2015 the number of notifications on personal data processing rose by 18% over 2014. A total of 9389 notifications of processing or changes to processing of personal data arrived at the Office, of those 1002 notifications (more than 10%) contained incomplete or inaccurate information or there were justified concerns that the notified processing could lead to violation of Act No. 101/2000 Coll. In such cases the notifiers were sent a request to amend the notification of personal data processing. Of the total number of entities to receive such requests, only 141 sent in additional information that confirmed the concerns of possible violation of Act No. 101/2000 Coll. and a suggestion for the commencement of proceedings under Section 17 of the Act was submitted. Of the total number of such suggestions, however, the processing of personal data was not permitted for only two notifications. For the others, the controllers altered the parameters for processing personal data or withdrew their registration, or in some cases adjusted the processing so as not to be subject to the obligation to register.

In addition to assessing the registration notifications received, the Office also issues decisions on the revocation of registration pursuant to Section 17a (2) of Act No. 101/2000 Coll. In 2015 a total of 106 processings were revoked at the controller's request, with the most frequent reason being the folding or merging of the company, dissolution of business activities, or terminating the processing of personal data. In three cases personal data processing registration was revoked based on the results of an inspection by the Office.

According to Section 19 of Act No. 101/2000 Coll., a controller recorded in the register is obliged to announce to the Office how it handled personal data after it terminates its activities. As this obligation is generally not met on the part of controllers, the Office used information from the Register of Persons and Register of Inhabitants to remove the entries concerning entities that no longer exist from the register of personal data processing. In 2015, 2694 registered controllers were removed from this register in this manner.

The most frequently submitted notifications of personal data processing concerned personal data processed by camera systems with recording and personal data processing as part of operating online shops.

In connection with the development of information technology, special methods of processing carried out through these new technologies are turning up increasingly often. This includes biometric systems used as part of security measures to check persons entering buildings or certain workplaces, for checking access rights when working with a computer, or attendance systems.

In terms of attendance systems it is always necessary to distinguish whether sensitive biometric data (e.g. fingerprint scans) is really being processed. The vast majority of biometric systems today work with templates, meaning the image is converted into a string of numbers. According to the opinion of the Office no. 3/2009, biometric data is not considered sensitive data if the biometric data (e.g. fingerprints) is unilaterally converted into encrypted strings of binary numbers from which the biometric information (e.g. fingerprint) cannot be reproduced.

Since there has been a rise in the number of submissions concerning the processing of personal data through biometric systems where it is not clear whether the notifier is working with real biometric data or just with templates, the Office has expanded the form for personal data

processing notification to include an additional form which is meant to advise the notifier whether it is truly processing biometric data or not. The goal of the amended registration form is above all to reduce the notifier's administrative burden, precluding subsequent correspondence in order to clear up ambiguities in the notification.

As in previous years, the trend continued of personal data processing in the form of publishing audiovisual records of municipal assembly meetings on websites. In the registration proceedings the notifiers in most cases declared that they will process the personal data of representatives and other public officials without their consent on the basis of the provisions of Section 5 (2)(f) of Act No. 101/2000 Coll., while the personal data of third parties contained in the agenda will not be processed or will be rendered anonymous.

With Act No. 64/2014, amending Act No. 101/2000 Coll., Section 16 of this Act was amended to include a new paragraph (6), which governs the situation whereby a controller submits a notification of personal data processing and at the same time an Office inspection of the controller is commenced or is underway. In order to prevent two proceedings from being underway at the same time (registration and inspection), the new paragraph adjusts the procedure of the Office so that entry into the register will take place after the Office has completed its inspection of the controller and determines the actual state of personal data processing.

Based on the emergence of new powers and new obligations, the Office prepared a new section on its website ("Notification according to Act No. 127/2005 Coll.") with links to legislation, a form for fulfilling the notification obligation and definitions of certain terms and procedures for notifiers. The form created by the Office is primarily meant to serve notifiers and thus facilitate the fulfilment of the obligations arising from Act No. 127/2005 Coll. The form also contains all the requirements that must be notified to the Office so it can assess a given notification.

After four years of experience it can be stated that obligated entities fulfil this legally stipulated obligation only sporadically (two cases of notification in 2012, one in 2013 and two in 2014; in 2015 the Office did not record any notification). The situation is similar in the majority of EU Member States, where there are only several submissions a year, with the exception of the Netherlands (348 notifications in 2015). There is some debate in the EU over the reasons for such a low number of notifications (6 October a meeting was held on the topic by the working group under the European Commission on data breaches, which meets once a year and which an Office representative also attends). One of the main reason for the lack of interest of controllers to report breaches is the fear of notifiers of possible sanctions if they admit that the security of personal data at their company was breached. There is also increased discussion of the effectiveness of reporting breaches in relation to increasing the level of security.

• TRANSFERS OF PERSONAL DATA ABROAD

In 2015 the Office ruled on 28 requests for an authorisation to transfer personal data to third countries according to Section 27 (4) of Act No. 101/2000 Coll.

Of the 20 authorisations issued in 2015, the most frequent basis on which the Office issued the authorisation were the provisions of Section 27 (3)(b) of Act No. 101/2000 Coll., as the applicant had created sufficient specific guarantees for personal data protection in the third country, always through approved Binding Corporate Rules (BCR). This was the case in nine instances.

Six times the basis for authorisation were the provisions of Section 27 (3)(e), i.e. transfer of data necessary for negotiating the conclusion or change of a contract made at the behest of the data subject, or for the performance of a contract to which the data subject is a contracting party. Four times, the legal basis for authorisation was Section 27 (3)(a), data transfer with the consent of or on the basis of an instruction from the data subject. In one case the Office issued an authorisation on the basis of the conditions laid down by Section 27 (d) and (f) of Act No. 101/2000 Coll. having been met.

In six cases the Office set the matter aside, generally on the grounds that in the end the applicant decided to rather deal with the transfer through an agreement including standard contractual clauses defined by a Commission decision. Two proceedings were suspended.

Aside from individual transfers of personal data to India, China, Southeast Asia and the Middle East, the marked majority of transfers were to the United States of America, which can be easily explained by the fact that many parent companies and headquarters of branches operating in the Czech Republic are located there. The majority of major companies providing information society services of various types, including cloud services, are also located in the United States.

The proposed solution, in terms of the demands placed on the transfer of personal data to third countries by the provisions of Section 27 of Act No. 101/2000 Coll., was found by the Office to be adequate.

The undoubtedly most significant event in the regulation of transmitting personal data abroad in 2015 was the October change in the system for transferring personal data to the United States. This change was caused by the Court of Justice of the European Union, which, in its judgment on case C-362/14 Maximillian Schrems v Data Protection Commissioner of 6 October 2015, declared invalid Commission Decision 2000/520/EC of 26 July 2000 according to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.

It was on the basis of this Decision, now annulled by the Court of Justice of the European Union, that the transfer of personal data to the United States to companies that had pledged to adhere to the Safe Harbour privacy principles had taken place under the provisions of Section 27 (2) of Act No. 101/2000 Coll., so that exporters of personal data did not have to apply for authorisation to transfer personal data to third countries according to Section 27 (4) of the given Act.

Doubts had long lurked among the ranks of the public and supervisory organs, however, as to whether the institution of Safe Harbour truly provided a guarantee of de facto and de jure protection of personal data transferred to the United States, as evidenced by the conclusions of analyses of the institution of Safe Harbour in practice (Safe Harbour Decision Implementation Study), which were drawn up in 2004 and again in 2008 at the request of the European Commission.

Following Snowden's revelations regarding the monitoring programmes in the United States (PRISM and others), under which the blanket transfer of data on EU citizens was being passed via internet companies to US public authorities, the aforementioned doubts culminated in a lively discussion, including at the EU level.

In this atmosphere the public activated as well. Maximillian Schrems, an activist in the protection of personal data, filed a complaint and asked the Irish Data Protection Commissioner to suspend the transfer of personal data to the United States to a company recorded in the Safe Harbour programme in accordance with Article 3 of Commission Decision 2000/520/EC. The Irish Commissioner rejected the complaint with reference to Commission Decision 2000/520/EC, which declared that the Safe Harbour programme provides an adequate level of personal data protection, so the Commissioner did not have the power to declare otherwise.

The Irish Supreme Court, which is dealing with the appeal by Maximillian Schrems, asked the European Court of Justice for a preliminary ruling on whether a supervisory body is bound by the Commission Decision on the Safe Harbour programme in assessing a complaint according to which the US does not ensure adequate protection for data subjects, or whether it can conduct its own investigation. The Court of Justice of the European Union responded to this question by saying that the Safe Harbour programme cannot exclude or limit the powers of national supervisory authorities to supervise compliance with personal data protection legislation.

At the same time, the Court of Justice of the European Union stated in the above judgment that the Commission in its Decision 2000/520/EC did not deal at all with the issue of whether the US legal system, on the basis of its internal regulations or international commitments, could ensure a level protection for fundamental rights that is essentially equal to the protection guaranteed within the EU on the basis of Directive 95/46/EC. The Commission did not investigate this, but limited itself to an assessment of the "Safe Harbour" programme. For this reason in particular the EU Court of Justice declared Decision 2000/520/EC invalid.

The Office reacted to the given Decision with the recommendation that was published on the Office's website. Over the course of October 2015 it also sent out communications with recommendations to all approx. 220 personal data controllers whose registered notifications on personal data processing pursuant to Section 16 of Act No. 101/2000 Coll. showed that they could be transferring personal data to US companies registered in the Safe Harbour programme.

In these recommendations the Office states that it is currently necessary to secure the transmission of personal data to the United States that is absolutely necessary for the fulfilment of the stated purposes through other instruments by which it is possible to ensure a corresponding level of personal data protection in third countries with an insufficient level of personal data protection, the most suitable of which would appear to be standard contractual clauses or binding corporate rules.

If the personal data controller transfers personal data to the US on the basis of a contract of which standard contractual clauses as per the below Decisions of the European Commission are an integral part, such transfer will take place under the Section 27 (2) of Act No. 101/2000 Coll., and the Office need not be petitioned for authorisation within the meaning of Section 27 (4) of Act No. 101/2000 Coll.

Potential further measures arising from the above decision of the Court of Justice of the European Union of 6 October 2015 will be implemented by the Office in coordination with the supervisory authorities of other EU Member States.

• SCHENGEN COOPERATION

In 2015 the Office actively fulfilled its obligations stemming from EU regulations governing the demands for supervision in terms of Schengen cooperation. Aside from supervision and monitoring of the now already fixed extensive information systems, which include the second generation Schengen Information System (SIS II), the Visa Information System (VIS), Eurodac and Customs Information System (CIS), the Office also dealt with the creation of information systems that are new from the perspective of planned future personal data processing. One example for all is the Entry/Exit System, focused on processing the personal data of third country nationals entering the European Union by its external borders. With regard to the amount of personal and sensitive data processed in such types of system, it is essential to ensure a corresponding level of protection of the data subjects' rights. Observance of the principle of personal data protection represents a primary prerequisite for the functioning of information systems under Schengen cooperation. In 2015 this was an area that was particularly put to the test as a result of the growing number of illegal border crossings.

News in the area of Schengen cooperation

In order to ensure the efficiency of individual coordination groups, 2015 was dominated by preparations for joint inspection models, which will lead to a unification of the procedures of individual countries participating in the information systems. The Czech Republic was chosen to act as rapporteur in preparing the joint inspection format for the Customs Information System.

In mid-2015, Regulation No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of "Eurodac" for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member States responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice came into force. In contrast to the original wording, the new legal treatment also applies to persons who have been granted subsidiary protection. In this respect the Office particularly welcomed the tightening of system's security guarantees and the elimination of the phenomenon of "asylum shopping" (a foreign national's application is processed simultaneously or successively by several Member States to which the foreigner purposefully moves).

The task of authorities for protecting personal data under Schengen cooperation also consists in supervising the proper exercising of the rights of data subjects, in particular the right to access data. With regard for this the Office took part in updating the Guide for Exercising the Right of Access under SIS II. In it the basic procedures associated with exercising the right of data subjects in all states of the Schengen area are clearly summarised. The document was then made available on the Office's website.

Current problems dealt with under the coordination groups

Biometric data, in particular fingerprints, represent the most reliable method of identifying a person in the case of third-country national visa applications, asylum applications, identifying certain categories of illegal immigrants, etc. Due to the rise in cases of counterfeit identification documents, scanned biometric data have gradually become the primary method of identification in practice for large-scale information systems. This fact has led to an increase in system capacity and automation of certain processes for capturing biometrics. For this reason the Office places emphasis on the issue of the quality of scanned fingerprints or photographs, including checking the training of responsible employees of personal data controllers. In this context we cannot forget compliance with the legal limits in the case of fingerprinting minors, the medically unfit, etc.

In keeping with tradition, in its supervisory practice the Office also focused on contractual agreements between personal data controllers and external service providers in the field of visa policy within the meaning of Article 43 of Regulation No 810/2009 of the European Parliament and of the Council of 13 July 2009, establishing a Community Code on Visas (Visa Code). As in such cases personal data processors do the work for controllers, it is essential to establish adequate limits for processing in the contract terms. From this perspective the Office does not consider it appropriate for the affecting outsourcing companies to also have access to the Visa Information System when collecting data from visa applications in light of the heightened security risk.

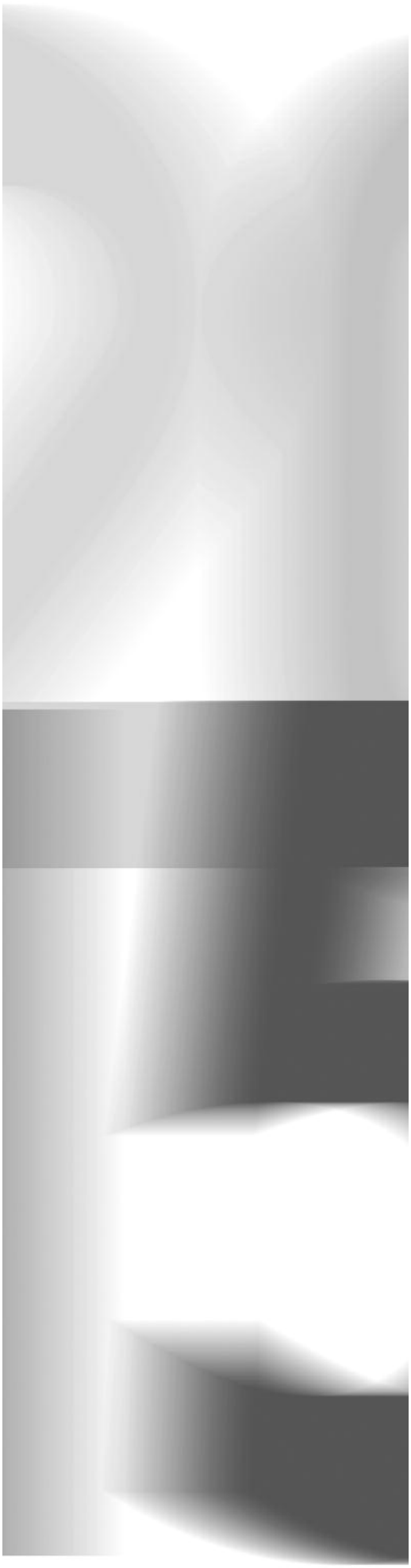
Number of instigations, complaints, queries and the handling thereof

In terms of the number of instigations received under Schengen cooperation, in 2015 the Office received a total of 11 concerning the processing of personal data in SIS II. All cases concerned exercising the right of data subjects to access data in SIS II, whether by exercising the right to information or exercising the right to have personal data deleted from the system. To this end the Office reviewed the actions of the personal data controller at the national level, which is the Police of the Czech Republic, and in no case did it find facts attesting to a violation of the rights of data subjects. Under this agenda the Office also received 48 submissions concerning the visa policy of the Czech Republic or the handling of visa requests, which however do not fall within its legally defined jurisdiction. For this reason the individual enquirers were referred to the Ministry of Foreign Affairs, under whose jurisdiction the given issue falls. In connection with this the Office clarified the competencies entrusted to it by Act No. 101/2000 Coll. as well as EU legislation.

Evaluating the level of personal data protection

Evaluation teams are always formed ad hoc for individual evaluations and are made up of representatives of the European Commission and experts from member states. Based on the submitted documents and an on-site inspection, which generally includes a visit to the police unit that provides for the national part of the Schengen database, the personal data protection authority and other affected authorities (the Foreign Ministry for the issuing of Schengen visas, the asylum office, the Interior Ministry as the competent authority for Schengen cooperation), the evaluation team prepares a report summarising its findings on the compliance of practice in the given Member State with the requirements of the Schengen acquis.

Over the past year employees of the Office were nominated as national experts for three evaluations. These were the evaluation of the level of data protection in Belgium (May 2015), Germany (June/July 2015) and Liechtenstein (November 2015).



Legislative activities

In 2015 the Office, as the commenting site for legislative consultation proceedings, was also a kind of guarantor that the drafts for plans and legislation included an evaluation of the impact on personal data protection and privacy in accordance with the legislative rules (DPIA). Aside from specific proposals and comments, the Office also intervened with a general warning in cases where the responsible ministries – the submitters of bills – had overlooked issues of personal data protection and privacy and instead of an expert assessment had included a political proclamation of the type, "*The proposed legislation fully respects the interest of personal data protection and does not in any way interfere with this interest*." In such cases the Office most frequently pointed out the absence of an evaluation of newly introduced information technologies and automated data processing, the misunderstanding of the mechanisms of data management and the inability to identify changes and potential risks in the processing and securing of personal data.

The Office's basic general comment is often the simple warning that if personal data are processed, particularly on the basis of a law, it always has an impact on the protection of privacy and personal data. The goal of the DPIA is not just an assessment of whether this impact is positive, neutral or negative, but rather an assessment of the method and risks of the proposed and existing processing of personal data. In the comment proceedings it is asked that the proposer clearly state whether the legislative proposal establishes new processing of personal data; if so, with what basic parameters, including but not limited to: specific purpose, category of personal data processed, the public or private nature of the processing, part thereof, or output from processing, and the retention period for personal data.

The absence of analyses of the proposed processing from the perspectives that are important for the protection of data (including personal data) tends to be most evident at first glance for technical material and non-legislative material. In the case of the Action Plan for Development of Intelligent Transport Systems, the Office called for clarification of the legal framework for the deployment of the technical means to process personal data and a description of the method of compliance as regards personal data protection and security.

In the following comment procedure for the amendment of Act No. 49/1997 Coll., on Civilian Aviation, the Office received a response that the issue of identifying unmanned aircraft and the obligation of their users (operators), including new standardised technical designs, will be "the subject of the current proposal of international experts and the European Commission", and for this reason the Ministry considers it "appropriate to take into account the more advanced form of this proposal in the future legislation".

DPIA is a mandatory component of amending acts if they introduce information systems. In the case of the central register of accounts, as a new fully digitised processing of personal data, the law lays out in detail the purpose of the processing of data in the register, the entities responsible for processing, the basic methods and means of processing, the retention periods, and the entities authorised to use data from the register. The Office pointed out the obligation to deal with issues of securing personal data according to Section 13 of Act No. 101/2000 Coll., which was completely omitted in the explanatory memorandum.

In the comment procedure on the draft amendment to Decree No. 357/2012 Coll. on the storage, transfer and disposal of traffic and location data, which expands the scope of stored traffic and location data for internet communication (electronic communication networks with packet switching and internet access services, identification of target devices), the Office requested that the expansion of items of data be compensated by shortening the period for which the traffic and location data on communication are retained.

The Office expressed a negative opinion on the plan to amend Act No. 582/1991 Coll., on the Organisation and Implementation of Social Security, adding a Deputy-initiated change to break the confidentiality of the Czech Social Security Administration (CSSA) laid down in Section 14 of Act No. 582/1991 Coll., and obliging the CSSA to share information with financial institutions in order to assess the ability of a consumer to repay a loan. The Office considered this bill non-systematic, in part, in addition to numerous practical reasons, due to the proposal to apply the consent of consumers to the processing of personal data in the public sector, as with regard to the constitutional principle of the legality of (execution of) state power, consent to the processing of personal data does not come into question for a public controller in its everyday agenda.

The Office had fundamental objections to the preparation and method of approval of an amendment that added an information database on the financial standing and credit history of consumers to Act No. 634/1992 Coll., on Consumer Protection. This was a complicated piece of legislation that was not prepared in the standard consulting procedure, i.e. on the basis of a government draft prepared by the competent ministry. The treatment of the aforementioned database is in essence a special law that has merely been formally inserted into Act No. 634/1992 Coll. As the legal treatment of the database was inserted into the act by a mere amendment proposal, the government did not comment on it and the bill did not receive the attention that such a fundamental matter deserves. Around the same time the government approved a draft Act No. 145/2010 Coll., on Consumer Credit, and the Chamber of Deputies discussed it as a separate item – that would have been a much more appropriate platform for regulating a consumer credit register. The Office pointed out a number of practical and legislative technical shortcomings in the draft, as the Deputy-initiated bill did not address fundamental legal obligations in the processing of data, from the legal reason (purpose) and principle of proportionality (substantiality) of processing personal data to the obligation to retain personal

data only for the period necessary. The Office requested that the overall objective – protecting the legitimate interests of providers – be the subject of public consultation with the stakeholders.

The above case attests to the fact that the rules of procedure for the Chamber of Deputies do not reflect Article 28 (2) of 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, transposed into Article 34 (7) of the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR) currently being prepared. European law here foresees that "Member States should consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of processing".

This problem comes up again and again, in 2015 for example in the case of a bill by a group of Deputies to add a provision to Act No. 99/1963 that "during the tour of the flat and its rooms, the one who is executing the decision shall make an audiovisual recording". At the time the bill was being discussed however it was clear that the existing legislation already allowed for the making of recordings and that the state supervision of executors has not mapped out what impact such measures would have in practice. The Office only found out about this bill from representatives of the Chamber of Executors of the Czech Republic, and debate on it in the Chamber of Deputies could not be considered transparent because at the time it was being debated it was not known who proposed the given provision and why, nor were there any records from the meeting of the relevant parliamentary committee.

The obligation to consult the preparation of legislation at the phase of legislative intent is prescribed by the government's legislative rules, but it lacks for private bills, particularly those initiated by Deputies. In recent years the Office has increasingly only been asked to directly (instead of the government or responsible minister) make a hastily prepared expert critique of a matter in the late phases of the legislative process by critics of a bill, which in most cases is impracticable with regard for the amount of time and limited information. In reality this means having to search for an emergency ad hoc solution, as there is too little time and very little room for designing and formulating the most appropriate legislation and it is necessary to focus solely on correcting the most serious and obvious errors. A fundamental, albeit only partial, solution to this problem would be adding to the Chamber of Deputies rules of procedure mandatory and timely requesting of a position from the Office if a bill concerns the processing and protection of personal data, or the Office's jurisdiction in general.

An example of the complex system of public administration where only one solution was drawn up in 2015 without any detailed evaluation of the options, was an amendment to Act No. 372/2011 Coll., on Health Services and the Conditions for Providing Them, that changed the National Health Information System (NHIS). This was an adjustment to the system introduced by an amendment to the Act on Public Healthcare. NHIS was not discussed with the Office when it was "moved" into the new Act No. 372/2011 Coll., and the Office's suggestions during preparation of the law were not taken into account at all. The Office's objections and its comments could thus only be properly implemented in 2015, when they were discussed directly with the new management of the Institute of Health Information and Statistics of the Czech Republic (IHIS). The Office took under advisement the positions of both the Health Ministry and IHIS as the guarantors of the amendment that no other form of changing the NHIS is

possible and its objective is to get the NHIS up and running so that it is meaningful and functional and then place it on completely new foundations by preparing a special NHIS Act within two years of approving the current amendment. Based on the Office's comments, the recitals of the amendment were added to so that room be made through "NHIS reform" for the monitoring and evaluation of the effectiveness and proportionality of the existence of NHIS as a whole and its component parts. The Office still holds that the whole reform of NHIS should undergo a deeper expert defence process.

In view of the above cases it can be summarised that at a time when internet services are on the rise and public administration is increasingly digital, it is very difficult to deal with practical issues of privacy only at the phase of comment proceedings on a bill. The Office is only able to provide consultation at this phase, and generally only for specific and detailed solutions presented for comments and drawn up by the expert team of the competent ministry. EU law, from which the legal protection of personal data stems, only provides principles, fundamental rights and obligations for personal data processing; the choice of manner and means in the case of public law is generally a matter for national legislation. The Office as a supervisory authority cannot fully replace the timely preparation of mechanisms for processing, not through consultation nor through inspection.

Foreign affairs and international cooperation

The Office's international activity was largely concentrated on modernising personal data protection in the European Union. As part of preparations for the reform package, the Office prepared or commented on the discussion material and positions for negotiations within the working groups and committees. The second important area of foreign activity was activity in the WP29 working party. Experts from the Office took part in the work of this advisory body for the European Commission in the specialised subgroups. The Office has permanent representation in four subgroups: the International Transfers subgroup, the Applicable Law subgroup, the Technology subgroup and the Borders, Travel and Law Enforcement subgroup. The Office also exercised its voice at regular WP29 plenary sessions (in 2015 there were five regular and one extraordinary plenary sessions). At the December plenary sessions, the heads of the various national authorities discussed the work programme 2016–2018. Debate was also launched on transformation of the WP29 working party into the European Data Protection Board, as foreseen by the prepared general regulation on protection of individuals with regard to the processing of personal data and on the free movement of such data, the approval of which is expected in spring 2016.

Of the number of documents issued by WP29 in the year in question, worth mentioning is the opinion on aspects of privacy and data protection issues relating to the utilisation of drones and the final report of an analysis on the policy for use of "cookies" by selected websites (in the private and public sector), in which the Office took part. The Office often uses these materials in its decision-making and consulting practice. It can be added in this context that the Office issued its own opinion on unmanned aircraft back in 2013 (Position No. 1/2013 – Processing of personal data via recordings from cameras on unmanned aircraft).

The Office was also active within the Council of Europe, primarily in working on modernising the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). The decision of

the Council of Ministers to invite several states that are not members of the Council of Europe to accede to Convention 108 will play an important role in the decision-making practice on international transfer of personal data. Specifically Uruguay, Morocco, Mauritius, Senegal and most recently Tunisia will be classified as countries providing an adequate level of personal data protection and it will no longer be necessary to apply for an authorisation to transfer personal data there.

In the field of bilateral relations, aside from standard cooperation in the form of consultation and swapping experiences with partner authorities, a two-day study visit of employees of the Albanian authority to Prague took place. The trip was funded and logistically provided for by TAIEX. Office employees shared their experiences, particularly in conducting checks and inspections. Their Albanian colleagues were also interested in the role of the Office in the legislative process, and there were discussions on the international transfer of data and protection of personal data in the world of the media.

The Office sent its delegation to traditional annual events (Spring Conference of Data Protection and Privacy Commissioners, International Conference of Data Protection and Privacy Commissioners, Conference of Central and Eastern European Data Protection Commissioners), which represent the top gatherings of their kind and offer a unique opportunity to make new work contacts and swap findings and experiences. The Office was also represented at the International Conference on Unmanned Aircraft Systems.

As in previous years, Office representatives worked in specialised supervisory and coordination groups set up under Europol and in connection with the operation of the Schengen Information System, the Visa Information System, the Customs Information System and the Eurodac database. Office employees were also members of teams set up for the purposes of Schengen evaluation.

The Office, media and communication tools

The primary communication tool was the Office's website. The general public can acquaint itself with current issues the Office is dealing with mainly in the sections Opinions of the Office / On Current Topics and Press Releases and Conferences. New technologies such as RSS channels or subscribing to updates have simplified the accessibility of information being sought. Press releases are sent to the Czech News Agency as well as both general and specialised print and electronic media outlets, and audiovisual media.

There was great media attention associated with the imposing of a fine of CZK 1 500 000 to CZK 1 900 000 to the companies eMarketing CZ s.r.o. and Traffic7 s.r.o. for sending unsolicited commercial communications. The record high fines were imposed for repeated distribution of commercial communications; in the first case the amount of the fine took into account the fact that the company had to have been aware that its actions were unlawful due to prior inspection and administrative proceedings against it. The fine was reported on by general media as well as specialised outlets such as lupa.cz, podnikatel.cz or the ČT24 programme @online.

Media interest was also associated with the appointment of the new President of the Office, JUDr. Ivana Janů, former Vice-President of the Constitutional Court and a judge on the International Criminal Tribunal for the former Yugoslavia. Ivana Janů was appointed as President of the Office by the President of the Czech Republic, Miloš Zeman, at Prague Castle on 26 July and on 1 September she got acquainted with the inspectors and various unit heads at the Office headquarters accompanied by the President's Chancellor Vratislav Mynář.

The print and electronic media also paid considerable attention to other topics, for example the Supreme Administrative Court judgment from February 2015 on the Ryneš case, the Municipal Court in Prague judgment on the ekolo.cz case, the introduction of camera systems and chips into schools in connection with the tragic incident in Žďár nad Sázavou and camera systems at football stadiums. In connection with the legislative process, media interest was attracted by the debtor registers and the amendment to the Insolvency

Act in connection with the newly introduced obligation (as opposed to the current option) of making a recording of distrainments, about which the Office expressed its misgivings. Regional media were interested in the case of the publishing of the names and birth dates of several thousand regional waste payers in Lovosice, for which the Office issued a fine. Special media attention was given to the conference on 15 years of the existence of the Office, which took place 6 June 2015. In a broader, international context, the most media attention went to the annulment of the European Commission Safe Harbour decision by the Court of Justice of the European Union. The Office published on its website a recommendation for personal data controllers on alternative ways of securing the transfer of personal data to the USA.

SPREADING KNOWLEDGE ABOUT PERSONAL DATA PROTECTION

In June 2015, the Office for Personal Data Protection commemorated the 15th anniversary of its creation. To mark this occasion it organised a conference along with the Czech Senate. The introductory block featured Igor Němec - President of the Office up until August 2015, Bohuslav Sobotka - Czech Prime Minister, Miroslav Antl - Chair of the Senate Constitutional Law Committee, and Radek Holeček - Chair of the Chamber of Deputies Privacy Sub-Committee. Presenting in the following block, entitled "Personal Data Protection and Today's Society", were President of the Supreme Administrative Court Josef Baxa, Public Defender of Rights Anna Šabatová, Josef Vacula, an inspector at the Office, and Jaromír Novák, Chairman of the Board for the Czech Telecommunication Office.

The first afternoon block, entitled "Personal Data Protection in Information Society", featured František Korbel of the law firm Havel, Holásek & Partners, independent journalist Jiří Peterka, Helena Svatošová of the NGO Iuridicum Remedium, Dan Jiránek of the Union of Towns and Municipalities, and Petr Hampl of Charles University. The last block, "Quo Vadis Data Personata Protectio?" contained the presentations of Karel Neuwirt, President of the Office 2000–2005, Jana Rybínová, an inspector from the Office, Hana Štěpánková, the Office's spokesperson in 2000–2014, and Miroslava Matoušová from the Department of Legislation and International Relations. A special issue of the Information Bulletin (No. 2/2015) was published to mark the occasion, which is also available on the Office's website and which features printed transcripts or summaries of the individual contributions.

Also included was a joint press conference, with the media focusing primarily on the speech of Prime Minister Bohuslav Sobotka, who praised the work of the Office and reminded people of the importance of a competent authority that makes sure the personal data of Czech citizens is protected. The media also reported on the most important activities of the Office over its 15 years of existence, during which it performed 1878 inspections, over 1200 administrative or misdemeanour proceedings, more than 31 000 consultations and queries, which most frequently focused on camera systems, insufficient security or leaking of personal data, copying of identification documents, and harassment by unsolicited commercial communications, of which the Office receives nearly 8 000 a year. The highest fine ever issued during the existence of the Office was the three million CZK fine for insufficient securing of personal data, due to which the data of as many as 700 000 insurance company clients were stolen.

In terms of spreading knowledge about personal data protection, the Office made use of publications and lectures. In 2015 it issued four positions available on its website. These are

Position No. 1/2015 – Operating a camera in a motor vehicle with a shot outside the vehicle, Position No. 2/2015 – Scope of data in published contracts, Position No. 3/2015 – Processing of personal data in connection with the keeping of medical records, and Position No. 4/2015 – Publishing contracts concluded between health insurance companies and medical service providers.

In 2015 the Office published a methodology dealing with the issue of the manner in which a customer is, or should be, informed in general terms and conditions on the processing of personal data when concluding and performing a contractual relationship. The methodology describes in detail and step-by-step how a given company should proceed in order not to violate Act No. 101/2000 Coll., and what the customer should watch out for when concluding a contract. It has come to light that clients are often robbed of their rights, put in a disadvantageous position or given incorrect information on their rights under general terms and conditions when concluding contracts, whether due to lack of knowledge of the law on the part of the company with whom the client is concluding the contract, or through deliberately unclear, unstructured formulation of the general terms and conditions, which can even lead to such provisions being invalid. The Office is attempting to use its powers to change this situation, both through inspections of individual business entities and through this newly published methodology, in which companies and customers alike can acquaint themselves with the rules of notification obligation and provision of consent to personal data processing.

Of the Office's print materials, Information Bulletin No. 1/2015, thematically focused on the issue of cookies in terms of internet privacy and the issue of the right to be forgotten, met with interest. The Office's official periodical, which is intended primarily for the professional public, is the *Věstník* [*Official Journal*], of which issues 69 and 70 were put out in 2015.

An important and integral part of awareness activity is lecturing, which a whole range of Office experts contribute to based on their specialisation. In 2015 Office employees lectured or gave conference talks in more than 50 cases. These were largely lectures for local governments (regional authorities, municipal authorities, municipal districts) and especially private and public benefit organisations, as well as interest groups and professional associations. In 2015 the Office had the opportunity to welcome European Commissioner Věra Jourová. The programme for the meeting was to inform each other on preparations for the EU regulation and activities in the field of personal data protection.

The Office also works to raise awareness among children and youth. To this end it declared the 9th year of the competition entitled "My privacy! Don't look, don't poke about!" to mark International Data Privacy Day, which was on 28 January. Children were to freely design a poster on the topic of personal data protection drawing attention to the currency of the topic of personal data protection. An alternative was to write a story, essay, script, make a video or to make a comic of a situation relating to personal data leaking from a database. Dozens of contributions came in in both categories, and they were evaluated by a jury made up of representatives of the Office and competition partners – Czech Radio, Association of Library and Information Professionals and SaferInternet. The authors of the winning contributions were invited to the Office headquarters, where they received prizes and an accompanying programme was prepared for them. A presentation on the experience of organising the competition was given in one of the panels at the International Conference of Data Protection and Privacy Commissioners by Office spokesperson David Pavlát who, along with the French

supervisory authority, helped prepare a practical guide for those agencies that do not yet have experience with this type of awareness activity.

OFFICE LIBRARY

The Office library is used primarily by Office employees, but also by students for term essays and theses concerning personal data protection. The collection of this specialised library grew in 2015 to include 62 new titles and 6 books the Office acquired by donation.

OFFICE WEBSITE

The Office website continues to be the main source of information for both journalists and the lay and professional public. Individual sections are steadily updated while maintaining an overview of the Office's prior actions. According to the government legislation rules, the Office is a mandatory comment site. It informs primarily the professional public of how it makes use of this position through the newly created section Legislation. During comment proceedings it pays particular attention to evaluating the impact of the proposed legal treatment on the relationship to privacy and personal data protection (DPIA). A new avenue of communication for the Office is Twitter, which it uses as an alternative way to distribute important information on its activities.

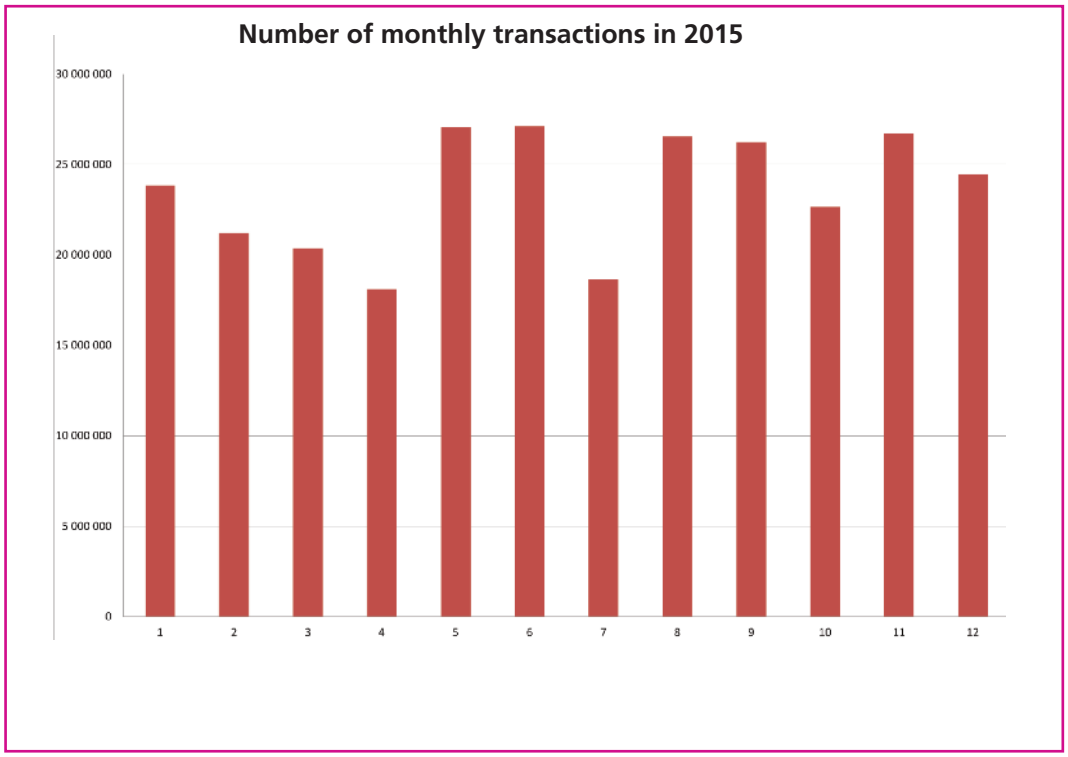
ORG Information System

The ORG Information System, which was created on the basis of Act No. 111/2009 Coll., on Basic Registers, has been up and running since 1 July 2012. This system fundamentally changed the approach to data that the state collects about citizens that it needs to function. Basic registers contain current reference data about citizens, legal entities, self-employed individuals and public authorities and thus simplify communication between citizens and the authorities.

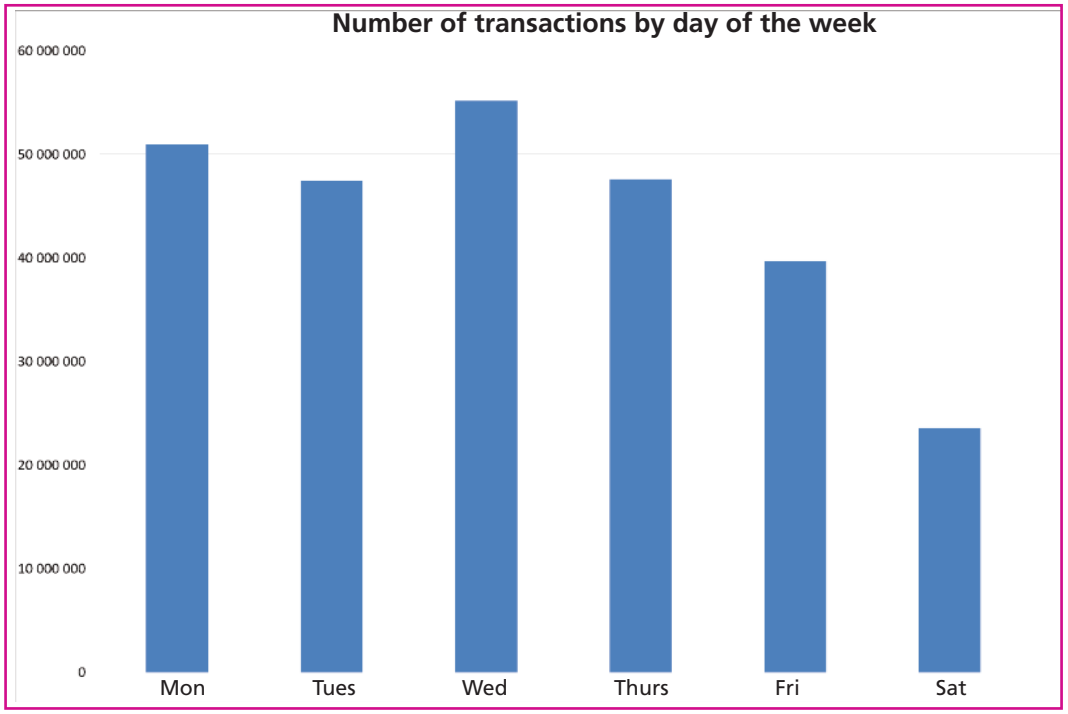
The system of basic registers stores the necessary data in registers. Data from these registers are accessible to authorised persons around the whole country. In order to increase the security and protection of data, the individual registers are managed by various authorities and bodies. Likewise the physical storage of data is spread around the Czech Republic for security reasons.

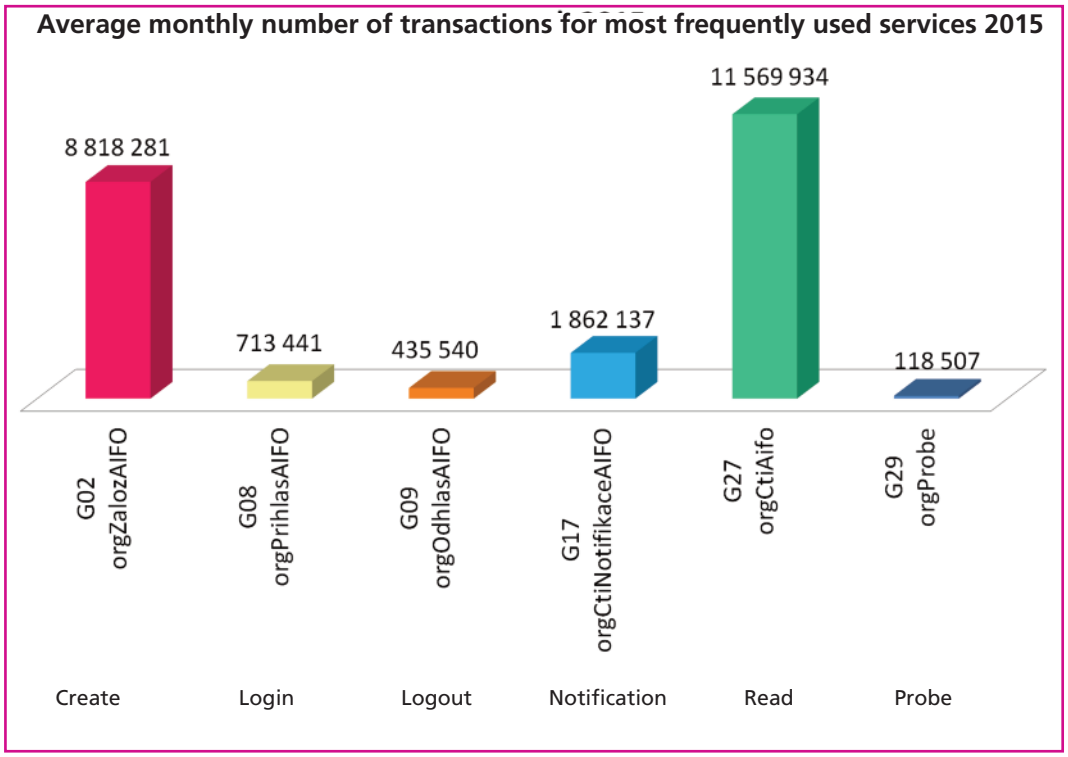
Under the System of Basic Registers, the ORG Information System was designated as an information system of critical information infrastructure in 2015 on the basis of Act No. 181/2014 Coll., on Cyber Security, since it contains data on all residents of the Czech Republic, and it is part of the e-government system.

As can be seen on the graph "Number of monthly transactions in 2015", the lowest number is in the month of April, when the daily number of transactions reaches 88% of the average daily number of transactions for the whole year. In contrast, in May and June the average daily number of transactions reaches 132% and in August and September 129% of the average daily number of transactions for the whole year. Comparing June and April, in June the average daily number of transactions is 150% of April levels. The growth in transactions in these months is likely related to the beginning and end of the school year at elementary schools and the associated items of parental benefits, social benefits, secondary school applications, graduations, etc.



The graph "Number of transactions by day of the week" shows higher activity on Monday and Wednesday. This is due to the extended office hours, or office hours for the public, on those days. In contrast the drop on Friday is likely caused by lower interest by citizens.





The ORG system processes various types of transactions, of which the most important are the transactions "ZalozAIFO" and "CtiAIFO", or "Create" and "Read".

Since the whole System of Basic Registers was launched 1 July 2012, more than 720 million transactions have been processed by the ORG system, which is an average of 600 000 a day, including Saturdays and Sundays. In 2015, the ORG system processed 282 909 267 transactions; the system was in heaviest demand in June, when 27 105 394 operations were processed.

Since ORG has been running, 380 public administration proceedings have been implemented into it and the ORG system processed 79 970 links to public authority information systems.

The whole system of basic registers is up 24 hours a day, 7 days a week. It is constantly being expanded and developed. Every citizen has used, uses and will use it, through public offices, when handling official matters or the official matters of their children.

In March 2015 a public inspection by the Interior Ministry's Structural Fund Department took place and an audit of the ORG Information System in the system of registers was performed under numbers 3/6133 and 4/6133. The auditors did not find any misconduct.

Office personnel

The number of job positions at the Office is determined by the State Budget Act for the respective calendar year, and effective 1 July 2015 also through the systemisation of service and job positions. In 2015 the number of systemised positions was 103.

Staff fluctuation in 2015 compared year-on-year increased slightly from 6% to 9%.

As of 1 January 2015, 99 employees were registered at the Office; as of 31 December 2015 the number was 101.

The average registered number of employees for 2015 was 99.01. Another 28 persons performed activities at the Office on the basis of non-employment work agreements.

The table "Breakdown of Office employees by age and gender" shows that the Office is dominated by employees aged 50 and older. In addition to suitable education, these employees also have long years of experience, with many of them employed at the Office since its inception, and they pass their experience on to new employees who are brought in when positions are freed up. Two thirds of the functional positions at the Office require a university education, while the remaining third of functional positions require completed secondary school education.

Economic management of the Office

The Office budget was approved by Act No. 345/2014 Coll., on the State Budget of the Czech Republic for 2015.

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

	in CZK thousands
Summary indicators	
Total income	4 277,64
Total expenditures	143 799,40
Specific indicators – income	
Total non-tax, capital income and accepted transfers	4 277,64
of which: total income from EU budget not including CAP	2 409,71
other non-tax and capital income and accepted transfers in total	1 867,93
Specific indicators – expenditures	
Expenditures to ensure performance of tasks of the Office for Personal Data Protection	143 799,40
Cross-sectional expenditure indicators	
Employee salaries and other payments for work performed	48 535,11
Mandatory insurance premiums paid by the employer *)	16 269,59
Contribution to the Cultural and Social Needs Fund	466,48
Salaries of employees in an employment relationship	27 277,14
Salaries of civil servants	10 669,11
Salaries of employees derived from salaries of constitutional officials	8 702,22
Total expenditures co-financed from the EU budget, not including CAP	13,59
of which: from the state budget	0,00
contribution from the EU budget	13,59
Total expenditures recorded in the information system for the EDS/SMVS funding programme	15 532,01

*) Social security and state employment policy premiums and health insurance premiums.

Details on the economic management of the Office will be presented in the draft state final accounts for the Office for Personal Data Protection, which is submitted every year in accordance with Ministry of Finance Decree No. 419/2001 Coll. (on the scope, structure and deadlines of data submitted for drawing up the draft state final accounts and on the scope and deadlines for drafting the final accounts for state budget headings) to the Ministry of Finance, the Supreme Audit Office and then to the Petitions Committee of the Chamber of Deputies.

INTERNAL AUDIT

The Office's internal audit plan for 2015 prescribed three audit investigations.

Audit of accounting document circulation at the Office

The objective of this audit was to check and evaluate the situation in the area being audited in terms of the internal regulations that set the rules for circulation of accounting documents under the internal control system and compliance with the valid legislation; to check and evaluate compliance of the objective functioning of the established system for circulation of accounting documents with the internal regulations of the Office particularly in the context of early detection; to evaluate and minimise potential risks in connection with the audited area, above all in relation to the form used for electronic preliminary management checks.

Audit of proper public procurement procedure

The objective of this audit was to check and evaluate the public procurement process in terms of compliance with the valid legislation with the goal of minimising operational, financial, legal and other risks that could arise in connection with fulfilling the approved plans and objectives of the Office; to check and evaluate the functionality and effectiveness of the internal control system from the perspective of the internal regulations of the Office that govern public procurement; above all to verify the performance of preliminary management checks (i.e. the phase before the contract is signed), including organisational securing of procurement processes at all phases. The audit also aimed to detect vulnerabilities in the procurement process as the basis for bringing internal regulations in line with Act No. 137/2006 Coll., on Public Procurement, and Act No. 320/2001 Coll. on Financial Control.

Audit of internal control system

The objective of this audit was to check and evaluate the situation in the audited area from the perspective of the proportionality and effectiveness of the internal control system and its compliance with the valid legislation, in particular with the relevant provisions of Act No. 320/2001 Coll. and the implementing Decree No. 416/2004 Coll. It also aimed to check and evaluate the ability of the Office's internal control system to catch, evaluate and minimise operational, financial, legal and other risks arising in connection with the fulfilment of the approved plans and objectives of the Office (Section 25 (1)(b) of Act No. 320/2001 Coll.). The audit also checked the implementation of recommendations from previous audits and proposed recommendations to remedy detected shortcomings and eliminate potential risks at the Office.

During realisation of all audits, emphasis was placed on checking compliance with all legal and internal standards, the existence of an aware risk management process at the Office was checked, as was the proportionality and effectiveness of the management and control mechanisms of the audited processes. The situation in the audited areas was in line with the generally valid legislation and Office's internal regulations in terms of the established procedures. Only insignificant deviations from the established standards and procedures were detected over the course of the audits.

In accordance with the Act on Financial Control, the Office submitted an annual report on the results of the financial inspections for the previous year to the Ministry of Finance in the stipulated form and by the deadline.

FINANCIAL STATEMENT

Approval of the final financial statement for 2015 and information on its transfer will take place by the standard deadline of 31 July 2016 in accordance with Annex 4 to Decree No. 383/2009 Coll., on account records in technical form of selected accounting units and their transfer to the central system of state accounting information and on the demands for technical and mixed forms of accounting records (Technical Decree on Accounting Records).

In accordance with the communication of the Ministry of Finance on the application of several provisions of Act No. 221/2015 Coll. amending Act No. 563/1991 Coll., on Accounting, and in connection with Act No. 101/2000 Coll., the Office is not obliged to have its financial statement approved by an auditor.

Provision of information pursuant to Act No. 106/1999 Coll., on Free Access to Information

In 2015 the Office received a total of 75 requests for information. This is a number comparable to the previous year, which confirms the sustained interest of the public in information concerning the Office's powers, particularly as regards the performance of supervisory activity.

Of the total number of requests for information, the Office obliged 52 of them in 2015, in 23 cases it rejected the information request partially and it did not completely reject any request. The most frequent reason for partial rejection of an information request was protection of the personal data contained among the requested information, in particular protection of data on third parties, damaged parties and witnesses in proceedings conducted by the Office. In such cases the requested documents were made available in an anonymised form.

Decisions on partial rejection of information requests were not challenged by appeals even once in 2015, which are directed to the President of the Office. Nor was the procedure for handling information requests the subject of any complaints under Section 16a of Act No. 106/1999 Coll. As in previous years, the Office's procedure for handling information requests under Act No. 106/1999 Coll. was not the subject of judicial review in 2015, and the Office thus incurred no associated costs.

In terms of content, the information requests were most frequently directed at the decision-making practice of the Office and judicial review thereof, as well as consultation statements provided by the Office. Applicants requested either inspection conclusions, administrative decisions or statements and positions of the Office concerning a certain category of data controllers or a certain activity, information on judicial review of Office decisions, including the administrative actions and Office statements on them, or more information on proceedings that the Office commenced ex officio on the basis of their prior instigation. A lesser part of the information requests also related to the economic management of public funding by the Office, including questions on the salaries of senior staff.

Handling of complaints under Section 175 of the Code of Administrative Procedure

In 2015 the Office again dealt with complaints under Section 175 of Act No. 500/2004 Coll., the Administrative Procedure Code. According to this provision, interested parties have the right to complain to an administrative authority if they believe that the administrative authority has acted improperly or if public officials have behaved improperly. The provisions of Section 175 of Act No. 500/2004 Coll. serve to protect the rights of interested parties if the law does not provide them with other means of protection, meaning lodging an appeal or other extraordinary remedies.

In 2015 the Office dealt with a total of 38 complaints. In the majority of cases the complainants expressed disagreement with the handling of their prior submission addressed to the Office in which the complainant raised suspicion of unlawful handling of personal data. Such complaints were evaluated and dealt with as a complaint under Section 175 of Act No. 500/2004 Coll. Of the total number of such complaints, nine were found to be justified and two as partially justified. The remaining 27 complaints were found to be unfounded. In several cases the complainant directed their complaint against multiple units of the Office. In comparing the overall number of complaints with the prior year it must be stated that the number of complaints has remained practically the same.

In nine cases the complainants turned to the Office with complaints against the conclusions of the inspection procedures of Office inspectors or the procedure in the leading of an inspection by Office inspectors, with two of this total number being found justified and seven as groundless. In the former two cases, the complainant was informed that misconduct was found and of further steps taken on the matter. For the remaining cases the complainant was informed that after reviewing their complaint, no misconduct had been found.

In seven cases the complainants turned to the Office with a complaint against the actions of the Administrative Department, which on the basis of a new authorisation under Section 40a of Act No. 101/2000 Coll. began the practice of refraining from imposing a fine if the unlawful state is remedied

immediately after the breach of duty was detected. In all such cases the grounds which led the unit to refrain from punishment were reviewed, and in six cases the complaints were assessed as unfounded, and in one case as partially justified.

Twenty three complaints targeted the Public Relations Department, whose task it is to deal with complaints and suggestions addressed to the Office. The vast majority of complaints were submitted due to the complainants not agreeing with the handling of a prior submission where said submission had been set aside by the Public Relations Department without any further measures. If a complainant submits a complaint under Section 175 of Act No. 500/2004 Coll., the prior submission and the method by which the given unit handled it are investigated. In the case of the Public Relations Department, seven complaints were found to be justified and one partially justified. The remaining fifteen complaints were assessed as groundless. If, after reviewing the complainant's submission, a suspected violation of Act No. 101/2000 Coll. was found, the standard legal procedure followed, with these submissions being passed along to an Office inspector for an inspection, or to the Administrative Department to launch administrative proceedings for suspicion of an administrative offence or misdemeanour.

In all cases the competent Office unit was informed of how the complaint was handled, and if its actions were found to be incorrect or partially incorrect, it was called upon to adopt such measures so as to prevent the same mistakes from occurring in similar cases.

As in the previous year, not one of the total of 38 complaints targeted inappropriate conduct of public officials. It is very good to learn that the Office acts responsibly in dealing with submissions received, supervisory activity and in administrative proceedings, and particularly when handling such it communicates with the public in protecting their rights and legitimate interests in accordance with the principles of good governance.

2015 Annual Report of the Office for Personal Data Protection
Office for Personal Data Protection
Pplk. Sochora 27, 170 00 Prague 7
E-mail: posta@uoou.cz
Internet address: www.uoou.cz

Based on the obligation imposed on it by Act No. 101/2000 Coll.,
on Personal Data Protection, Section 29 (d) and Section 36,
the Office for Personal Data Protection published this
Annual Report on its website in February 2016.

Editor: PhDr. David Pavlát, tel. no. 234 665 286
Copy editing: BcA. Květa Gebauerová, DiS.
Graphic design: Eva Lufferová
Proofreading: Mgr. Eva Strnadová
Printed by: Tiskárna Helbich, a. s., Valchařská 36, 614 00 Brno
Published for the Office for Personal Data Protection by Nakladatelství MU Brno, 2016

ISBN 978-80-210-8144-4