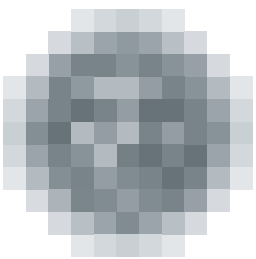
Annual Report Summary 2016



úřad pro ochranu osobních údajů
the office for personal data protection

Foreword by the Office President

Ladies and gentlemen,

I would like to present for your kind attention the Annual Report of the Office for Personal Data Protection (hereinafter the Office) for the year 2016. Aside from the fact that it was the first year that I could start to implement my own notions for change in the activity of the Office and the results of these changes began to appear, it was also an initiation year in terms of the further evolution of personal data production. The reason for this is that the long-planned change to the legal framework for personal data protection has entered into force in the form of a new EU General Data Protection Regulation and associated regulations, though it does not yet apply. This harmonises personal data protection in the 28 EU Member States and is a fundamental quantitative and qualitative shift that preserves the original legal foundations and principles. The Office has already begun systematically and conceptually preparing for the upcoming changes. This is a continuous, dynamic and ongoing process of a getting acquainted with the new legal treatment, analysing and interpreting the new legal institutions and preparing for application in practice. Other entities at the national and EU level are also addressing this process responsibly.

The new legal framework enshrines the need for more thorough and effective protection of personal data, or more broadly of privacy in general. One of the most current topics of the day stems from the development of new

technology and data streams that work with personal data, provoking concerns among natural persons in particular as to whether their data are being sufficiently protected. According to current statistics, 80 percent of Europeans believe that their data are not protected enough. Significant then in this regard is the right to informational self-determination, enshrined at both the level of EU law and our own constitutional order, which consists of the right of an individual to decide whether, to what extent and whom to provide access to their personal information. This right may only be restricted by law. Privacy and personal data protection run inherently counter to the right to access to and dissemination of information, much as a similar tension can be seen in the relationship between individual privacy and security of the state. In order to resolve these conflicts of rights, it is necessary to apply proportional reasoning in the decision-making process, with an assessment being made in several steps as to whether the infringement on a fundamental right serves a legitimate goal and whether it is absolutely necessary and commensurate. The situation must always be assessed with a view to all the circumstances and specifics of the given case. In some cases this comprehensive assessment has already led to a re-evaluation of certain earlier approaches of the Office, including several positions. Court rulings have also helped clear up certain controversial issues, allowing certain points of departure to be clarified. The Office has ceased to adopt negative positions or publish opposing statements to the press on the rulings of courts, which it did in the past. The Office respects the case law of courts and develops its arguments, thereby properly reflecting its function as an administrative body protecting individual privacy as a fundamental right. These changes are also reflected in the evaluation of submissions to the Office, the conducting of inspections and in administrative proceedings, including in the Office's approach to the subject of the most frequent complaints received, which is camera systems.

In terms of specific changes, partial reorganisation of the Office was prepared and launched back in 2015. The major objective of this was to support the work of Office inspectors, specifically concentrating the inspection activities carried out in the state service system under the Supervision Department, which should lead to the creation of appropriate conditions for harmonising decision-making procedures. Aside from this internal organisational change, which was only fully felt in 2016, I would like to draw attention to the visible changes of the Office's external policy, in particular in informing the public. To put it simply, we are trying to communicate with the interested public more and more actively. Our primary medium in this regard is the Office's website. Since last year, for example, reports are published every six months on all inspections completed by Office inspectors, whereas no such complete summary used to be provided.

It is no doubt worth mentioning that the Public Relations Department, which is an important consultation body for the professional and general public, received a total of 4721 submissions, questions, complaints and consultation requests in 2016; of these 143 were passed along for inspection or administrative proceedings.

Of the more than sixty administrative proceedings under the Act on Personal Data Protection, the general public will no doubt have heard about the fine of CZK 3.6 million levelled against T-Mobile for the leak of customers' personal data.

The legislative unit recorded that, despite the generally improved cooperation with submitters of (nearly two hundred) legislative proposals, the Office was, in contrast to the past, only left out as a consultation point several times. This was the case for the proposed amendment

to the Act on the Intelligence Services of the Czech Republic, in which a reform of supervision of the intelligence services was proposed.

For the sake of completeness I shall also point out that the Office conducted a public consultation on online cameras, which followed up on an extensive round-table discussion. This is a complex topic hiding a number of sub-issues with limited possibilities to apply the existing Personal Data Protection Act (in the absence of a special act on camera systems). The Office is also publishing all available information as preparation for the application of the new General Data Protection Regulation. We are also making use of the results of joint work between the supervisory authorities of EU member states, which we are gradually attempting to become more involved in and contribute to.

Last but not least, we managed to implement another of my goals, which was setting up an analytics unit. The basis for legal and analytical work is working with all available and relevant background materials, in particular legislation, national and international court rulings, comparative studies and expert literature. Analytic work provides room for reflection and evaluation of existing and planned legal regulation of personal data protection, including its relationship to other areas of legislation. This activity essentially helps demarcate the direction of the Office's decision-making while respecting the boundaries between analytical findings and inspection activities. The goal is to seek out optimal solutions to complex issues of personal data protection.

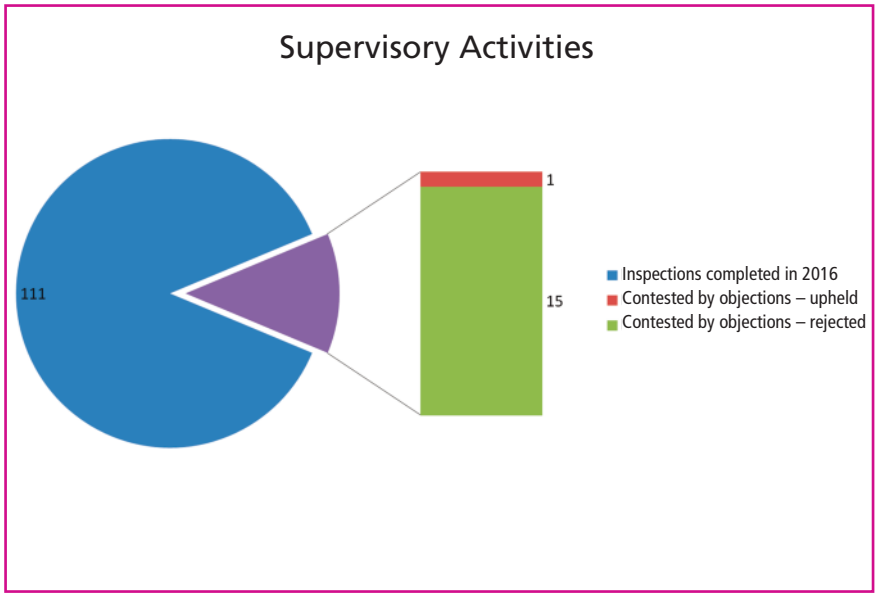
In conclusion I would like to state that while in the first months of my tenure at the head of the Office I noticed that problems with the protection of privacy and personal data were viewed in the public debate as specific situations and isolated incidents, after the approval of the EU's general regulation, which will take effect in May 2018, the situation began to change. The Office is no longer alone, as other entities must also deal with the "agenda" of personal data protection.

I trust that these activities will ultimately help achieve the aim pursued by the Office, which is protecting the privacy and personal data of natural persons in a digital and technologically demanding (revolutionary) age, the centre of which must remain service to humanity.

Ivana Janů
President of the Office for Personal Data Protection

Contents

Supervisory Activities



I. SUPERVISORY PLAN

The Office's supervisory activities are conducted on the basis of a supervisory plan, the initiative of the Office President, and tips or complaints that alert it of violation of Act No. 101/2000 Coll.

All inspections are run by Office inspectors with the support of the Supervision Department, which was set up 1 January of this year by dividing the original Section of Supervisory Activities.

The Office's inspections focused on areas where it was possible to expect a higher level of risk in the processing of personal data, as well as areas where prior experience had shown that there could be systemic errors or improperly set conditions for the processing of personal data.

In 2016 the Office focused on the processing of personal data carried out by public administration in the context of large volumes of data (Big Data),

where such data is further used for purposes such as marketing. The objective was to check whether the selected entity was not further using personal data from legally processed databases for other purposes.

The Office also focused on the compliance of responsible entities with obligations in using "cloud computing" services. Cloud service customers should conduct a comprehensive analysis of the risks associated with the utilisation of such services, including the cross-border transfer of personal data, particularly to third countries that do not ensure an adequate level of protection. All providers of cloud services should furnish their customers with all information concerning transfer and the location of data storage so that the customer can properly assess all the advantages and disadvantages of the provided service.

At a selected development company an inspection was conducted on the conditions for protection of personal data in connection with preparation and implementation of development projects during installation and operation of surveillance systems. The processing of personal data within systems that use biometric data for employees to enter areas where work takes place was also not ignored. Certain special legal conditions need to be upheld when processing sensitive data, which include biometric data.

In the field of electronic communication, a supervisory aim was to check whether confidentiality was being ensured technically and organisationally for messages and associated operating and location data that are transferred via the public communication network and publicly accessible electronic communications systems.

Also included in the supervisory plan was an entity against which supervisory or administrative proceedings were conducted in the past concerning Act No. 480/2004 Coll., on Certain Information Society Services and Amending Certain Acts (Certain Information Society Service Act). The inspection focused on the observance of the conditions for sending commercial communications as well as observance of the Personal Data Protection Act.

In 2016 the inspectors conducted the following inspections in keeping with the supervisory plan:

1. The processing of personal data in connection with the **use of traffic and location data** provided to the Police of the Czech Republic, where the inspected entity was the Ministry of the Interior – Police of the Czech Republic – Regional Directorate for the City of Prague Police. The inspection is being run by inspector František Bartoš. The aim is to examine all facts related to the use of traffic and location data provided to the Police of the Czech Republic pursuant to Act No. 127/2005 Coll., on Electronic Communication and Amending Certain Related Acts (Electronic Communication Act), and the observance of the conditions for processing such under Act No. 101/2000 Coll. and Act No. 273/2008 Coll., on the Police of the Czech Republic.

   The inspection had not been completed in 2016.

2. The processing of personal data carried out by public administration in the context of large volumes of data (**Big Data**) and the further use of such data for purposes such as marketing. The inspected entity was the Czech Statistical Office (hereinafter "CSO"). The inspection was run by inspector František Bartoš. The subject of the inspection was to check the observance of the principle of legality in processing personal data sourced from CSO

databases which are, or are to be, subsequently used for the commercial activities of that entity.

The inspection was launched in May 2016 and completed in September 2016. No violation of Act No. 101/2000 Coll. was found by the inspection.

3. **Utilisation of data from the Population Register** on the basis of legal authorisation. The inspected entity was a selected health insurance company – Škoda Employee Health Insurance Company. The inspection was run by inspector Božena Čajková. The inspection was focused on compliance with the conditions laid down by Act No. 101/2000 Coll. in processing the personal data of insurees. The inspection found that the inspected entity processes a number of personal data of insurees, including data obtained from public administration information systems, as these are also active in the field of public health insurance pursuant to Act No. 48/1997 Coll., on Public Health Insurance. The inspection checked whether the legal title of Article 5(2)(a) or (b) of Act No. 101/2000 Coll. could be applied to all personal data processing relevant for the inspection, i.e. that the personal data of insurees can be processed without their consent. The inspection also checked due compliance with the obligations of Articles 13, 14 and 15 of Act No. 101/2000 Coll. No violation of Act No. 101/2000 Coll. was found by the inspection. During the inspection the inspected entity modified its approach to data in basic registers while using the "e20" service, which is offered by the National Registers Authority.

4. **Processing under local government** – right of access to the Population Register. The inspected entity was a selected municipality, in this case the city of Říčany. The inspection was conducted by inspector Božena Čajková along with an inspection team. Inspected was the city's compliance with obligations in processing personal data from the basic register information system, in particular the Population Register (as well as from the information system on population records based on Act No. 128/2000 Coll., on Municipalities (the Municipal Order), and Act No. 111/2009 Coll., on Basic Registers). The inspection found that the city is a processor of personal data in relation to the registers in question, processing the personal data in order to exercise the devolved power of a municipality pursuant to special legislation. The inspected entity thus acted on the basis of a legal title under Article 5(2)(a) of Act No. 101/2000 Coll. The inspection also checked whether the inspected entity took appropriate measures to safeguard the personal data as per Article 13 of Act No. 101/2000 Coll. and addressed the obligation of confidentiality of employees in the city's internal regulations and employment contracts in accordance with the requirements of Section 15 of Act No. 101/2000 Coll.

5. **Surveillance systems in development projects**

The inspected entities were selected property development and construction companies. The inspection was led by inspectors Božena Čajková and Jiřina Rippelová.

The aim of the inspection was to check the conditions for personal data protection in connection with the planning and implementation of development projects when installing and operating surveillance systems in residential buildings and the immediate vicinity. In October 2016, two inspections were launched based on the supervisory plan: an inspection

of the Owners' Association of the Residential Centre building at Zvonařka 2536, which was led by inspector Čajková and which was not completed in 2016, and an inspection of the Owners' Association for the building at Čistovická 1700/62, which was led by inspector Rippelová and which did not find any violations of Act No. 101/2000 Coll.

6. Processing of personal data in churches and religious communities

The first inspected entity was the Ministry of Culture. The inspection was launched on the basis of the supervisory plan. The subject of the inspection was compliance with the obligations of a controller/processor of personal data laid down by Act No. 101/2000 Coll. when processing the (sensitive) personal data of data subjects, i.e. members or persons professing allegiance to a church or religious society in connection with their registration or keeping lists of registered churches and religious societies. The inspection was run by inspector Petr Krejčí. It focused on personal data processing in connection with operating an information system with a large volume of data, in particular sensitive data of persons professing allegiance to a certain church or religious society. No violation of the Act on Personal Data Protection was found in the inspection.

The second inspected entity were the members of the preparatory committee of a religious society, based on a tip from the Ministry of Culture in connection with a submitted application to register a religious society with said ministry, from which a suspicion arose that the members of the religious community's preparatory committee were violating the Personal Data Protection Act. The inspection was run by inspector Petr Krejčí. The suspicion stated in the tip was confirmed and violations of the provisions of Article 5(1)(g), Article 5(2), Article 9 and Article 11(1) of Act No. 101/2000 Coll. were found during the inspection.

The third inspected entity were further members of the preparatory committee of the religious society based on a tip from the Ministry of Culture. The inspection was run by inspector Petr Krejčí. In the given case, extensive cooperation of other entities had to be secured, as it was necessary to determine the actual state of things among the contradictory claims of the inspected parties, both for the purposes of the Office's own inspection findings and so that the inspection report could be used for the further administrative decisions of another administrative authority. This inspection turned up violations of the provisions of Article 5(1)(g), Article 5(2), Article 9 and Article 11(1) of Act No. 101/2000 Coll.

7. Transferring personal data to third countries

The inspected party, which is an entity providing services in the field of tourism, as part of which it transmits personal data to third countries, is the company Čedok, a.s. The inspection was launched in December 2016 and is being led by inspector Petr Krejčí. The aim of the inspection is to check compliance with the conditions for processing personal data in accordance with Article 27(3) of Act No. 101/2000 Coll. on the part of a responsible entity. The inspection, which follows up on the judgment of the European Court of Justice on case C-362/14 Maximillian Schrems v. Data Protection Commissioner, has not been completed.

8. Processing of personal data of visa applicants

The inspected entity was the Ministry of Foreign Affairs – Consulate General in New York. The inspection was run by inspector Petr Krejčí. The intention of the inspection was to check

compliance with the obligations of a responsible entity in processing the personal data of visa applicants for short-term and long-terms stays in the Czech Republic. The inspection was launched in May 2016 and completed in September 2016. The inspection did not find any violation of Act No. 101/2000 Coll.

9. Archiving and filing services

   The inspected entity was the National Archives. The inspection was run by inspector Jiřina Rippelová. The subject of the inspection was the processing of personal data transmitted to the National Archives by the Czech Statistical Office under Article 22(4) of Act No. 296/2009 Coll., on the 2011 Census. In March 2014, the inspected entity received from CSO partially anonymised census forms filled in by obligated persons during the census (i.e. the Personal Census Sheet, Flat Sheet and Building Sheet). The CSO carried out anonymisation by removing (blacking out) certain data. On the Census Sheet however, data which in the opinion of the Office could be identifiable for certain natural persons were not anonymised (e.g. a combination of data on the municipality, part of the municipality and specific employment, or on an ethnic minority, uncommon mother tongue, membership in a less common church, or data on an uncommon number of children, in association with a year of birth).

   The inspecting entity thus stated that contentious data listed in the Personal Census Sheet form are personal data in the sense of Article 4(a) of Act No. 101/2000 Coll. and in some cases also sensitive data pursuant to Article 4(b) of this act (data attesting to whether a person lives in a registered partnership and data on nationality or religious beliefs of the data subjects). The inspection found that the personal and potentially sensitive data in question are being processed by the inspected entity in accordance with Article 5(2)(a) and Article 9(ch) respectively of Act No. 101/2000 Coll. and it was stated that the inspected entity had adopted such technical and organisational measures as to take into account the purpose and means of personal data process and which guarantee the required level of personal data protection.

10. Processing of personal data using surveillance systems that utilise biometric data

    The inspected entity was the company Skanska a.s. The inspection was led by inspector Jiřina Rippelová. The aim of the inspection was to check available evidence concerning the installation of biometric identification of persons entering the inspected entity's construction site using FaceID technology. The inspected entity checked the manner in which the obligations of responsible entities were observed for processing of personal data, including biometric data, which are classified as sensitive data. According to the inspection findings and other available information, the inspected entity uses these groups of information with the help of special software to identify persons entering the area where construction work or related activities are taking place. The inspection was launched 5 April 2016 and completed 30 September 2016. The inspection did not find any violations of Act No. 101/2000 Coll.

11. Processing of personal data in upholding the Czech Republic's obligations in the field of international police cooperation

According to Article 9 of Council Decision 2009/371/JHA on Europol, each member state is obliged to establish or designate a Europol National Unit in charge of carrying out designated tasks. The Europol National Unit is the point of contact between Europol and the competent national authorities of the member states. The inspected entity was the Ministry of the Interior of the Czech Republic. The inspection was run by inspector Daniel Rovan. The aim of the inspection was to check the procedure and manner by which the obligations of a responsible entity were observed for personal data processing when transferring and providing access to them as part of international police cooperation. The inspection was launched 16 May and completed 31 August 2016. The inspection did not find any violations of Act No. 101/2000 Coll.

12. Electronic communication

An inspection in the field of exercising supervision focused on checking and assessing the observance of obligations of responsible entities in sharing and providing access to confidential information of participants or users in terms of the legality of their conduct in connection to Article 89 of the Electronic Communications Act and Position of the Office No. 6/2013, Provision of Information on Traffic and Location Data Stored by Operators of Electronic Communications Services. The inspected entity was the company O2 Czech Republic a.s., which is one of the entities that provides publicly available electronic communications services. The inspection was run by inspector Daniel Rovan. The inspection, which began in September 2016 and was completed in December 2016, did not find any violations of Act No. 101/2000 Coll.

13. Healthcare

The aim of the inspection was to check compliance with the conditions for processing personal data by state administrative authorities in the protection of public health and other entities which take part in such processing.

The inspected entity was the Regional Hygiene Station in Brno. The inspection, which was run by inspector Jana Rybínová, was launched 30 September 2016 and has not yet been completed.

14. Education

Inspector Jana Rybínová set as the aim of this inspection checking the observance of conditions for processing personal data by the Ministry of Education, Youth and Sport of the Czech Republic and any other potential entities taking part in processing. The inspection was launched 21 March 2016 and is still underway.

15. Observance of obligations of responsible entities in utilising "cloud computing" services

Part of the supervisory plan for 2016 was to carry out an inspection that focuses on realising the conditions for protecting personal data under Act No. 101/2000 Coll. concerning the obligation of a controller or processor when processing personal data using clouds, in particular as regards the conditions for securing the processed personal data. The inspected entities are: Česká spořitelna, a.s., MONETA Money Bank, a.s., and Sberbank

CZ, a.s. All the inspections, which are being run by inspector Josef Vacula, were launched in December 2016.

16. **Observance of obligations of responsible entities under Act No. 480/2004 Coll.**
The supervisory plan for 2016 also included an inspection pursuant to Act No. 480/2004 Coll. focused on the conditions to be observed for sending commercial communications, as well as under Act No. 101/2000 Coll. concerning the obligations of a controller or processor in processing personal data in connection with its business activity.
The inspection was launched on 1 June 2016 and the inspected entity is the company AAA Auto International a.s. The inspection, which is still underway, is being led by inspector Josef Vacula.

17. **Processing of personal data while utilising data obtained in connection with the operation of road traffic surveillance systems by the Police of the Czech Republic**
When installing and operating traffic surveillance systems, these systems are made available and information is drawn from them for the needs of the Police of the Czech Republic. The aim of the inspection was to check the legitimacy of the subsequent utilisation of these data and observance of the conditions for processing thereof under the conditions of Act No. 101/2000 Coll.
An inspection of the Regional Police Directorate for the Liberec Region was launched 7 September 2016 and completed 23 September 2016. The inspection did not find any violation of Act No. 101/2000 Coll. An inspection of the Ministry of the Interior – Police of the Czech Republic was launched 19 October 2016 and has not yet been completed. Both inspections were led by inspector František Bartoš.

II. FINDINGS OF INSPECTORS FROM SUPERVISORY ACTIVITY

This chapter lists the findings from the key inspections. A complete overview of the results of supervisory activity is given on the Office's website in the section Dozorová činnost / Zveřejňování informací o kontrolách (Supervisory Activity / Publication of Information on Inspections) – in Czech only.

Inspection of management of visual medical records at healthcare facility Perfect Clinic s.r.o. (inspector Jana Rybínová)

The subject of the inspection at the healthcare facility Perfect Clinic s.r.o. (hereinafter the "Inspected Entity" or the "Clinic") was compliance with the obligations laid down under Chapter II of Act No. 101/2000 Coll., with a focus on observance of obligations in processing personal data while providing health services, especially the processing of personal data in connection with the keeping of medical records and the securing thereof pursuant to Article 13 of Act No. 101/2000 Coll.

The reason for the launching of the inspection was a tip that the Office received from a complainant stating that they had noted a number of facts over the course of health services provided by the Inspected Entity based on which they suspected that the Inspected Entity as a provider of health services had systematically and for some time been failing to uphold its obligations laid down by the legislation, in particular Act No. 372/2011 Coll., on Health Services and the Conditions for Provision Thereof, but also Act No. 101/2000 Coll. The complainant believed that the Inspected Entity was not keeping any systematic measures to secure the safety of processed personal data as demanded by Article 13 of Act No. 101/2000 Coll. The attending physician made photographs of the patient (surgical site) with his private mobile phone, and even several months later had not placed them in any secured storage device belonging to the Clinic.

The inspection revealed that the Inspected Entity is a healthcare facility and provides healthcare on the basis of Act No. 372/2011 Coll., thus the purpose and means for its processing of personal data are laid down by the provisions of Article 53(1) of the aforementioned act, according to which a healthcare facility is obliged to keep a patient's medical records and manage them in accordance with that act and other legislation. Medical records are a set of information pursuant to paragraph 2 of the aforementioned provision of the act that apply to the patient about which they are being kept. Within the meaning of Article 4(j) of Act No. 101/2000 Coll., the Inspected Entity is a controller of personal and sensitive data of patients.

The complainant underwent a total of three surgical procedures at the Inspected Entity, with photo documentation being taken by the attending physician as part of all the associated health services provided. At that time however the Inspected Entity had no internal directive in place governing the handling of visual documentation, this issue being dealt with with employees verbally. In the case of the healthcare provided associated with one of the surgical procedures, the attending physician took multiple photographs of the complainant with his mobile phone in April 2013, only transferring these photographs from the surgical procedure

into the Inspected Entity's database in October 2013. It was found that the Inspected Entity did not have complete disposal of five photographs of the complainant from at least April 2013 until October 2013. The storage of the pictures in the memory of the mobile phone did not provide sufficient protection against destruction, unauthorised access and transfer; such a manner of storage must be considered highly risky. It was also found that one of the photographs related to the provided healthcare associated with a surgical procedure in December 2013 was still not part of the complainant's medical records in April 2015. The Inspected Entity thus did not have complete disposal of the photograph taken of the complainant from at least December 2013 until May 2015.

In conclusion the inspector stated that at least in the aforementioned periods the Inspected Entity was processing medical records of the complainant that were not complete, as they did not contain the photo documentation made during the provision of health services (a total of six photographs), which happened as a result of the lack of an internal regulation documenting and governing a regulated approach in taking photographs of clients and the management thereof, as the submitted internal directive "Photo Documentation of Clients" did not exist. Thus in the above period the Inspected Entity had not adopted such measures as to prevent the unauthorised processing of the personal (sensitive) data of the complainant, thereby violating the provisions of Article 13(1) of Act No. 101/2000 Coll.

It was furthermore found that the medical records archive of the Inspected Entity is located in the underground garage of the building, entrance to the archive is from a separate unlocked corridor, the door to the archive is not secure, is not equipped with a safety lock, no camera system is installed in the corridor or the archive itself and records are not kept of the documents stored in the archive. The inspector stated that the Inspected Entity had not adopted sufficient technical and organisational measures within the meaning of Article 13(1) of Act No. 101/2000 Coll. so as to sufficiently secure the medical records stored in the archive, since as a result of insufficient technical and organisational measures it has not secured complete disposal over the medical records stored in the archive, thereby violating the provisions of Article 13(1) of Act No. 101/2000 Coll.

The Inspected Entity submitted objections against the inspection findings, stating that the taking of photos for aesthetic surgery is purely at the discretion of the attending physician. Photo documentation is always made with the knowledge and consent of the patient. If photographs were taken of a patient by the physician with a mobile phone, this was an exceptional situation in which the Clinic's camera was abnormally not available and it was necessary to take photographs during the examination. The physician used a work telephone owned by the Clinic and the photographs were transferred to the company's protected data storage after having been taken and erased from the mobile phone. There was neglect and delay on the part of the physician whereby the photographs were not uploaded to the complainant's medical records immediately. The physician faced consequences from the Clinic for this individual misconduct, being punished for violation of his responsibilities, and the Clinic immediately explicitly instructed all employees and associates to exclusively and without exception use the designated camera for taking photos of patients, with any potential violation of this regulation to be punished by the Clinic. In its objection the Clinic also stated that it is not true that the photographs were kept outside the complainant's medical records until 2 October 2013. The Clinic also stated that it always had complete disposal over all photographs of all patients taken

during examinations for the purposes of inclusion in the patients' medical records. As regards the securing of the medical records archive, the Clinic argued that it is currently intensively addressing the possibility of more thoroughly securing the archive (securing the door, a camera system), including potentially moving it to a different space. Making records of the documents stored in the archive is already underway. The company has thus adopted the first measures to rectify the identified shortcomings and is working to rectify the remaining ones.

The Office President, as the second-instance administrative authority, by decision of 11 March 2016, rejected the Clinic's objections and reaffirmed the inspection findings, i.e. violation of Article 13(1) of Act No. 101/2000 Coll.

As the competent administrative authority, the Office fined the company Perfect Clinic s.r.o. CZK 15 000 for committing an administrative offence under Article 45 (1) h) of Act No. 101/2000 Coll. as it had failed to adopt or implement measures to ensure the security of personal data processing.

Housing cooperative – operation of a camera system in buildings and records of access chips holders (inspector Jiřina Rippelová)

Based on a tip received pointing out shortcomings in the processing of personal data of residents of a residential building in connection with the issuing and keeping of records on access chips, as well as the operation of a camera system in the building, the Office launched an inspection. The Office thus carried out an inspection of the housing cooperative focused on compliance with the obligations of a personal data controller laid down in Chapter II of Act No. 101/2000 Coll., in particular the provisions of Articles 5, 11, 13 and 16 thereof.

The inspection found that in the residential building in question (made up of 280 residential units), a total of 31 cameras are installed which, however, have not yet been put into operation, i.e. are currently not recording and have not yet ever recorded and are not even in online mode. In terms of the camera system it was thus found that no processing of personal data is taking place and thus Act No. 101/2000 Coll. cannot be applied.

Operation of the chip system and associated keeping of records on allocated chips that allow their owners to enter the building was however confirmed and thus assessed in terms of compliance with the requirements of Act No. 101/2000 Coll. In particular it was found that the system in question is set up solely on the basic software level, meaning that the chip functions like a key, but no record of the number of the chip used is taken in relation to the date and time of entry. Thus no processing of personal data of the natural persons to whom the chips have been allocated is taking place in association with the chip system and there is no reason to evaluate compliance with the obligations arising for a personal data controller or processor under Act No. 101/2000 Coll.

The housing cooperative does however keep records of all persons to whom a specific access chip to the building has been issued in association with operation of the chip system. According to the inspection findings, chips were issued to members of the cooperative and members of their households, as well as to other persons who lived in the building and furthermore to persons whom a flat tenant intended to allow access to the building (relatives, acquaintances, subtenants, etc.). At the time of the inspection approximately 1200 chips had already been issued and the housing cooperative had collected and kept records of these persons' personal data in order to block a specific access chip in the case of loss or theft so that unauthorised persons could not access the building.

The housing cooperative chose the approach that it only issued chips to applicants in the case that each applicant for a chip filled out a form on handover of the chip for access to the building, in which they stated their personal data including name, surname, the number of their ID card or other identifying document, permanent residence address, mailing address, telephone number and signature. To these data the housing cooperative added the number of the assigned chip and the date it was issued. Part of the form to be filled out was a statement whereby the chip applicant gave the housing cooperative consent to the processing of personal data in the above scope.

If the chip applicant refused to provide the above personal data or refused to sign the consent to personal data processing, the housing cooperative refused to issue the entry chip and referred such persons to the possibility of entering the building by doors where a key system was left in place. Although one such set of doors was left in each of the three sections of the apartment building, it is evident that this measure hampers the access of persons who refuse to provide the cooperative with the requested personal data.

This approach by the housing cooperative was assessed as going against the requirements expressed under Article 5(1)(d) of Act No. 101/2000 Coll., i.e. that the housing cooperative was collecting personal data that were not essential to fulfil the stated purpose. In the opinion of the Office it would be fully sufficient for fulfilling this purpose (determining the assigned code if an access chip is lost or stolen, erasing it from the system so a foreign person could not enter the building, and issuing a new access code to the person in question) to process the personal data of a residential unit tenant to the extent of unit number, name and surname of tenant, number of chips handed over including their registration numbers, date of issue and the signature of the tenant. The housing cooperative was processing the other personal data of flat tenants and all other personal data of persons living in the apartment building (or visiting said building) in violation of the law.

In the opinion of the Office, specific processing of personal data must always be judged according to the specific personal data controller, the purpose it has laid down and the specific circumstances of the given processing. If the purpose laid down by the housing cooperative for processing personal data is administration of entrance chips (including blocking specific chips in the case of loss or theft and allocating a replacement chip), it is not possible for such an extensive amount of personal data as was found in the inspection to be processed for this purpose. Administration of entryway chips could be ensured in the given case by other means, or by using considerably fewer processed data, thus with less infringement on rights of natural persons to protection of privacy.

In the case of the other obligations faced by personal data controllers under Act No. 101/2000 Coll. (e.g. under Articles 13 and 16 thereof), the inspection came to the conclusion that no misconduct occurred.

Over the course of the inspection the housing cooperative already took steps to partially rectify the situation found, yet it nevertheless submitted objections to the findings listed in the inspection report. The Office President did not however uphold the objections and the inspection was thus closed.

Based on the facts found during the inspection an order was issued by which the Office commanded the housing cooperative to take measures to rectify the shortcomings found. The housing cooperative was ordered to destroy the personal data which it was processing unnecessarily

according to the inspection findings (i.e. in violation of Act No. 101/2000 Coll.), specifically the personal data of all persons except flat tenants and information on such concerning the number of chips issued and code thereof. The housing cooperative carried out the measures ordered within the set 30-day deadline, of which it then informed the Office in writing.

For committing an administrative offence under Article 45(1)(c) of Act No. 101/2000 Coll., the Office imposed a fine of CZK 80 000 on the housing cooperative.

Ministry of Labour and Social Affairs (hereinafter "MLSA" or the "Ministry") – fulfilment of the obligations of a controller in securing the personal data of benefit applicants and employees of the MLSA and Czech Labour Office (inspector Božena Čajková)

The inspection of MLSA and companies (Fujitsu and VITSOL) was launched at the instruction of the Office President in reaction to a suggestion from the National Security Office. This suggestion led to concerns about abuse of Ministry and Labour Office data stored in external data centres and the due return and irreversible erasure by the companies (processors under Act No. 101/2000 Coll.).

The MLSA acceded to an Implementation Agreement (a contract concluded between the Czech Interior Ministry and Fujitsu), based on which the contractual relationship was modified by gradual conclusion of addenda. The subject of the addenda was the company's commitment to provide the Ministry and Labour Office with services consisting of providing rental of computing capacity in external data centres, which not only ran information systems providing for the payment of non-insurance social benefits and state employment policy benefits, but also information systems for identity management and electronic record-keeping services for the Ministry and Labour Office. The company VITSOL then provided these services for Fujitsu.

From the content of the tip there arose a concern that upon termination of the contractual relationship between the Ministry and the companies, the backed up data in the external data centres could be misused and may not be properly returned and irreversibly erased. In order for the inspectors to eliminate the real risk, they issued a Decision on a Preliminary Injunction. The companies were thus ordered to refrain from and prevent any activity that would lead to modification or deletion of the data (personal data of social benefit applicants, employees and associated operating data of the MLSA and Labour Offices).

In connection with the above the inspection was focused on the fulfilment of the Ministry's obligations in securing the personal data of benefit applicants and employments, in particular the adoption of technical and organisational measures upon termination of the contractual relationship with the companies in terms of the returning of all stored data to the MLSA, Labour Offices and the irreversible erasure of personal data, as well as measures adopted in checking access to records of activity with the stored data in external data centres (logs).

At the data centres, the companies backed up (processed) a large range of personal data, not only the data of social benefit applicants that it is necessary to collect and further process in order to approve individual benefits (e.g. name, surname, maiden name, date and place of birth, birth number, residence address, telephone number, e-mail address, data mailbox number, ID card number, passport number, social system card number, bank account number), but also certain personal data of persons assessed along with the applicant for a contribution or benefit. Furthermore, in accordance with Act No. 329/2011 Coll. on the Provision of Benefits to Persons with Disabilities and Amending Related Acts, sensitive data about the health of

the applicant (disability) were also stored. In connection with the administration of the information systems for identity management and the electronic records service, other personal data (of MLSA and Labour Office employees) were also stored in external data centres.

According to Government Order No. 432/2010 Coll., on the Criteria for Determining an Element of Critical Infrastructure, the Ministry's information systems are numbered among the critical systems, and thus it is essential for the administrators of such systems to thoroughly uphold the obligations for securing personal data. If the Ministry as a personal data controller under Act No. 101/2000 Coll. entrusts the processing of personal data to a processor (the company), it must act in accordance with Article 6 of Act No. 101/2000 Coll. This provision of the act declares that: "*Unless the delegation arises from a legal regulation, the controller and processor must conclude an agreement on processing of personal data. This agreement must be in written form and must especially explicitly state to what extent, for what purpose and for what period it is concluded and must contain guarantees from the processor on the technical and organisational securing of personal data protection.*"

The inspectors assessed the content of the contractual arrangements between the Ministry and Fujitsu, in particular the Implementation Agreement and its successive addenda. Not only did these not contain guarantees by the company (processor) on the technical and organisational securing of personal data protection, they did not even address the specific procedures and measures of the parties in concluding a contractual relationship in connection with processing of personal data. The Ministry thus violated the cited Article 6 of Act No. 101/2000 Coll.

The inspectors furthermore focused on compliance with the Ministry's obligations in securing the personal data of benefit applicants and other assessed persons stored in the data centres. According to Article 13(1) of Act No. 101/2000 Coll., "*the controller and processor are 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.*" *According to paragraph (2) of the same provision,* "*the controller or processor is obliged to develop and document the technical and organisational measures adopted to ensure personal data protection in accordance with the act and other legal regulations.*" Paragraph (4) c) of Article 13 of the cited act obliges the controller or processor "*to make electronic records that make it possible to determine and check when, by whom and for what reason these personal data were recorded or otherwise processed*." The inspectors assessed the state of things and came to the conclusion that over the course of the termination of services with the companies, the Ministry did adopt sufficient technical and organisational measures within the meaning of Article 13(1) and (2) of Act No. 101/2000 Coll. in connection with the returning of back-ups and deletion of data.

According to the contractual arrangements with the companies, the Ministry did not have access to records on the activity of the processed data in the data centres (logs). On the part of the MLSA as controller, it was thus necessary to adopt measures pursuant to Article 13(1) of Act No. 101/2000 Coll. associated with regular inspection of rights to access the data stored in the data centres. The inspection found that during the contractual relationship, i.e. since accession to the Implementing Agreement, the Ministry did not carry out supervisory activities as regards the provisions of Article 13(4)(c), thereby violating obligations arising from Article 13(1) of Act No. 101/2000 Coll. and as a result losing ongoing control over the handling of production data stored in external data centres.

As part of the performed inspection, the inspectors also focused on the adoption of measures during the destruction of personal data at the data centres in connection with the termination of its contractual relation with the companies. The MLSA along with the companies set up a clear process for destroying the data and the inspectors found that the measures carried out, in which the MLSA took active part, precluded any misuse of the data before deletion thereof and the chosen method of deletion guaranteed a high degree of effective destruction of the data.

For committing an administrative offence under Article 45(1)(h) of Act No. 101/2000 Coll., the Office fined the Ministry CZK 150 000.

Inspection of the Statutory City of Plzeň (inspector Petr Krejčí)

The subject of this repeat inspection was observance of the obligations of a personal data controller-processor laid down under Chapter II of Act No. 101/2000 Coll. in connection with the processing of personal data obtained from applicants for a municipal flat who filled out an application form for the selection procedure who are declared the flat tenant before the conclusion of a contractual relationship, or during lease/sub-lease agreements to flats owned by the city where sensitive data was also demanded, in particular as regard (non-)conviction of a crime. The inspector conducted the inspection on the basis of a tip from the Deputy Ombudsman delivered to the Office for Personal Data Protection in September 2015.

Within the meaning of the provisions of Article 2 of Act No. 128/2000 Coll., on Municipalities (the Municipal Order"), the Statutory City of Plzeň, (hereinafter the "Inspected Entity") is a public corporation that has its own assets, acts on its own behalf in legal relationships and bears liability arising from such relationships, and also takes care of the overall development of its territory and the needs of its citizens; in fulfilling its tasks it also protects the public interest. One of the purposes of personal data processing is negotiations on a contractual relationship concerning tenants in individual buildings managed by the Inspected Entity. In particular the inspection relates to the notification of personal data processing in which the Inspected Entity gave notice of the processing of sensitive data indicative of a criminal conviction. The municipality argued that according to the provisions of Article 38 of Act No. 128/2000 Coll., the municipality's assets must be used effectively and economically in accordance with its interests and the tasks arising from its legally defined jurisdiction. The municipality is obliged to take care of the maintenance and development of its assets. The municipality's assets must be protected against destruction, damage, theft or misuse. The municipality's obligation is thus to protect its assets against unauthorised intervention and exercise its right to compensation for damages and right to disbursement of unjust enrichment in a timely manner. The municipality is obliged to constantly monitor whether debtors are fulfilling their commitments duly and on time and ensure that no statute of limitations or expiration occurs.

An application for selection of a tenant must be properly filled out in all the prescribed points. The participant delivers the application by the deadline stated in the plan. An integral part of the application is Consent to Processing and Publishing of Personal (Sensitive) Data pursuant to Act No. 101/2000 Coll. Without filling out the application and signing this consent, no lease agreement can be signed with the party interested in renting the flat.

It was this involuntary consent to processing and publishing of sensitive data that formed the basis of the Ombudsman's disapproval, especially the fact that a party interested in

a municipal flat who applies to the selection procedure and has a criminal conviction does not have equal conditions in such a competition.

As the Inspected Entity processes data on natural persons (applicants for a flat) – name, surname, title, birth number, permanent residence address, mailing address, telephone number, marital status, source of income and amount thereof, number of persons who will be using the flat along with the applicant, whether the person has or has not been convicted of an intentional crime and potentially also whether they are or are not working with a social or probation worker or parole officer – the data subject is definitely identified on the basis of such data and thus the data processed by the Inspected Entity can be considered personal data within the meaning of Article 4(a) of Act No. 101/2000 Coll.

According to the provisions of Article 4(a) of Act No. 101/2000 Coll., sensitive personal data means a personal piece of data that reveals national, racial or ethnic origin, political beliefs, membership in trade union organisations, religious or philosophical beliefs, criminal convictions, state of health and sexual life, or genetic data on the data subject; biometric data that allows direct identification or authentication of the data subject is also sensitive data.

The Inspected Entity demanded from applicants for a flat a solemn declaration whether their criminal record statement does or does not contain information on conviction of an intentional crime, with the applicant also appending to the solemn declaration a criminal record statement, solely for perusal and verification of the facts stated in the solemn declaration. If the criminal record statement does contain information on conviction of an intentional crime, the Inspected Entity demands written confirmation from a social worker, probation worker or parole officer of long-term cooperation (which has lasted at least six months), under which the applicant has actively cooperated in dealing with their life situation to change their previous way of life. In cases where the solemn declaration contains information that the applicant was convicted of a crime, such information in such a solemn declaration can be considered sensitive data. The written confirmation from the probation worker or parole officer can also be considered sensitive data. Probation workers must be visited by those who have been granted conditional release with probation supervision, i.e. the confirmation from the probation worker attests to the fact that the applicant has been convicted of a crime and the probation worker confirmation is thus sensitive data. Parole officers work with clients at all phases of criminal proceedings and afterwards, meaning during imprisonment or detention and after release. Confirmation from a parole officer can thus again attest to the fact that the applicant has been convicted of a crime and this confirmation is thus sensitive data.

On the basis of the provisions of Article 5(1)(d) of Act No. 101/2000 Coll., every personal data controller is obliged to collect only those personal data that correspond to the specified purpose and to the extent necessary to fulfil that purpose. When processing personal data, the controller must only collect a scope of personal data that does not lead to excessive processing of personal data. The Inspected Entity demands a mandatory solemn declaration from natural persons applying for a flat that their criminal record statement does not contain information on conviction of an intentional crime along with an appended criminal record statement, solely for perusal and verification of the facts stated in the solemn declaration. If the criminal record statement does contain information on conviction of an intentional crime, the Inspected Entity requires confirmation from a social or probation worker or parole officer. Processing of this sensitive data on conviction for any intentional crime by the Inspected Entity can be considered

superfluous information, as it is not apparent how the sensitive data on conviction for an intentional crime testifies in general about whether the applicant currently fulfils or will fulfil in the future its obligations to the Inspected Entity as a tenant, or its obligations to the state, and whether they violate or in the future in the case a lease agreement is signed that they will violate "good morals in the building", which the Inspected Entity considers the purpose of processing such sensitive data. The fact that the applicant has an entry in their criminal record for an intentional crime does not testify in any way as to their current behaviour and efforts to fulfil the obligations of a tenant of a flat owned by the Inspected Entity or their future behaviour towards other tenants of municipal flats or the Inspected Entity or the state. Even though the Inspected Entity has stated that, based on long years of experience and practice in renting out and managing flats, it considers it highly risky in terms of tenant obligations to allow an applicant that has already been convicted of an intentional crime to live in a flat, it did not substantiate in any way the claim that applicants whose criminal record contains an entry on conviction of an intentional crime would be a true risk for the Inspected Entity in terms of due payment of rent and utilities. From the perspective of the Inspected Entity, an applicant who has been convicted, for example, of accepting a bribe, bribery or damaging and threatening the environment, or for violating regulations on the rules of economic competition, which are intentional crimes, would be a risk in terms of due fulfilment of tenant obligations. Such a premise from the Inspected Entity can be clearly rejected as unfounded. It is possible to agree with the Inspected Entity that certain kinds of intentional crimes can mean an increased risk as regards fulfilment of tenant obligations, but what cannot be agreed with is that every flat applicant that does not prove they have not been convicted of an intentional crime is a potential non-payer of rent and a tenant that violates the "good morals and order in the building and its surroundings". Even the provisions mentioned by the Inspected Entity of Article 2288(1)(b) of Act No. 89/2012 Coll., the Civil Code, which give a landlord the right to give an eviction notice in the case that a tenant is convicted of an intentional crime committed against the landlord or member of their household or a person who lives in the building where the tenant's flat is, or against foreign property that is located in the building; the condition for giving notice applies only to a narrowly defined group of intentional crimes and not all intentional crimes as a whole. The purpose of processing sensitive data on conviction for an intentional crime stated by the Inspected Entity on such a general level has a significant impact on the scoring or classification of the flat applicant in the ranking of applicants for the flat, thus it cannot be considered personal data processing to the extent necessary to fulfil the stated purpose. If there are high-risk groups of flat applicants, this fact can be dealt with in another appropriate manner, e.g. in the lease.

By processing superfluous sensitive data on flat applicants that are not necessary in terms of the purpose, the Inspected Entity violated the obligations arising from the provisions of Section 5(1)(d) of Act No. 101/2000 Coll.

Loss of record sheets (inspector František Bartoš)

The Office received 15 original Record Sheets by postal carrier in a sealed postal envelope along with an accompanying anonymous letter stating that these documents were found in a public place.

It was determined that the Record Sheets were drawn up by the company Forcorp Group, s.r.o., (hereinafter "Inspected Person" or the "Company") for the year 2014 and contained

personal data comprising: name, surname, date of birth, birth number of insuree, maiden name, place of birth, address (street, house number, municipality, post office, post code), nationality, course of insurance in the given year (from-to, code, number of days insured, excluded periods, assessment base, date from which the company is registered). The Record Sheets were marked with the name of the employer, including the signature and stamp of the person responsible for producing them.

The Record Sheets are drawn up every year for all employees and are produced in two physical copies. One copy is intended for the Company's records, being stored for the given year in a separate Record Sheet register. The second copy is for the needs of the employee. Retirement plan Record Sheets are given to the employees for signature once they have been made, either in person or through the regional manager or they are sent by Czech Post. Both counterparts are always presented for signature. The inspection found that the Records Sheets are given to the employees to sign either right in the payroll department office or are sent out by the manager of the regional branches. It was also found that the Company did not keep any records of processed Record Sheets. Access to the office spaces where labour law documents are processed was not governed by any internal regulation and thus it was not possible to discover in any way when and how the loss took place.

The inspection found that the Inspected Entity did not have exact rules drawn up under its adopted technical and organisational documentation to secure personal data as regards security of individual offices and movement of persons in the building, including exact rules for records of documents contain employee personal data. The inspection established that the Company had not fulfilled the obligation of a personal data controller to adopt such measures so as to prevent unauthorised or accidental access to personal data or loss there, and it was unable to find out who had sent the Office Record Sheets containing its employees' personal data, when and how. Thus violation of obligations under Article 13(1) of Act No. 101/2000 Coll. occurred as a result of the fact that the inspected company had not adopted sufficient technical and organisational measures to protect personal data, thereby violating the controller obligation under Article 13(2) of Act No. 101/2000 Coll.

As part of the Office's authority, administrative proceedings were launched with the Company, imposing measures to rectify the shortcomings found within the meaning of Article 40 of Act No. 101/2000 Coll., specifically to draw up and adopt specific measures through internal regulations to ensure the safety of personal data, with exact specification of the purpose and scope of personal data processed and specific responsibility for this processing being assigned to specific employees in connection with the scope and purpose of the processed employee personal data.

Following up on the findings of the inspection, Forcorp group, s.r.o. was fined CZK 15 000 as part of administrative proceedings for violation of obligations laid down in Article 13(1) of Act No. 101/2000 Coll., i.e. the obligation 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 for committing an administrative offence under Article 45(1)(h) of the same act, as it had not as a controller adopted or executed measures to ensure the security of personal data processing.

Inspection of association Mamma HELP (inspector Daniel Rovan)

On the basis of complaints, an Office inspector carried out an inspection at the start of 2016 of the group Mamma HELP (hereinafter the "Inspected Entity"), the subject of which was a tip on the sending of requests for a financial contribution to contributors and persons and the associated processing, in particular the updating of the personal data of the contacted subjects, including the deceased. The complaints were submitted by relatives of deceased persons who saw this correspondence as insensitive and feel offended by this manner of obtaining financial support.

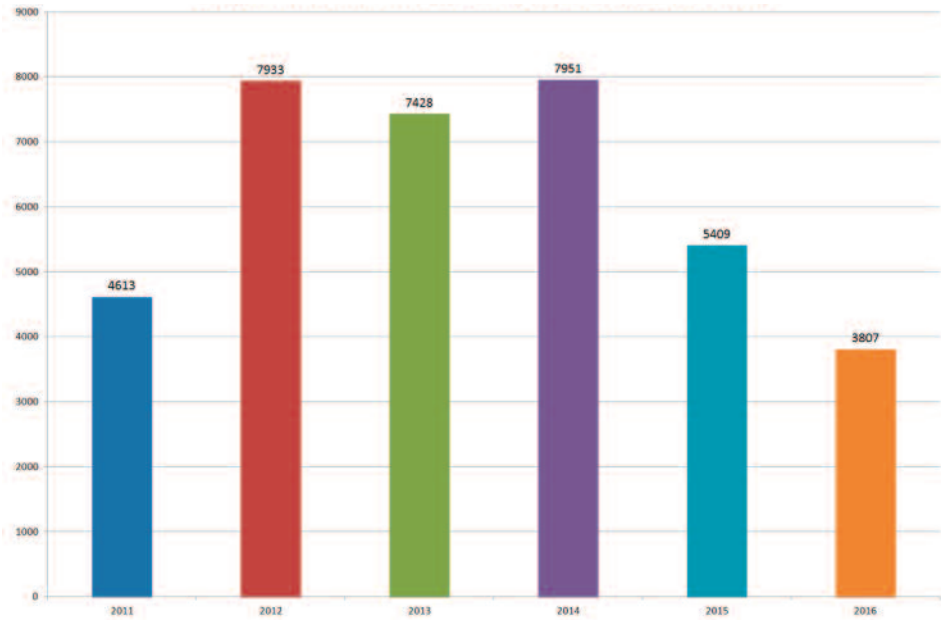
The inspection found that the Inspected Entity has an internal regulation drawn up for protecting personal data and its employees have demonstrably been acquainted with the regulation. It was also determined that the Inspected Entity does not carry out the selection of recipients (potential donors) itself. For this purpose it has a framework agreement concluded with the company prodialog, s.r.o., which provides direct mailing services for the Inspected Entity and in connection with this procures the addresses of potential donors, to whom it sends requests for financial support for Mamma HELP, z.s. It does so on the basis of an agreement on personal data processing, the subject of which is the processing of published personal data for the purpose of fundraising for the Inspected Entity on the basis of a framework agreement.

Mamma HELP does not come into contact with these addresses. Only in the case that the addressees react positively to the request for support and become donors are their personal data processed in the donor database.

The inspection checked the obligations of a controller within the meaning of Article 5(1)(c), Article 5(2) and Article 11(1) of Act No. 101/2000 Coll. Violation of Article 11(1) was found, that is the obligation to inform, as the data subjects were provided with erroneous information on who was the processor (change of business name, failure to include Registration Number) of their personal data, as the letters were marked with a partner company title and logo that were no longer current and which did not correspond to reality. They could thus have been confusing for the addressees, as they were being contacted by a de iure non-existent company. In light of the fact that the Inspected Entity already adopted rectification measures during the inspection and the violation did not comprise a significant invasion of privacy, no fine was imposed.

The inspection conclusions led to a subsequent inspection of another entity, the company prodialog, s.r.o., which was the contractual partner of Mamma HELP, z.s. at the time of the inspection. The inspection found violation of Article 5(1)(c), as prodialog s.r.o. had not updated the personal data of a specific person whose personal data had not been publicly accessible for several years already at the time of the inspection, and who as a result of this failure to update had been contacted as a potential donor despite the fact that she was no longer alive at the time of the letter. In light of the fact that the Inspected Entity already adopted measures to rectify the situation over the course of the inspection, and in light of the low danger to society, no fine was issued.

UNSOLICITED COMMERCIAL – NUMBER OF COMPLAINTS RECEIVED



The distribution of unsolicited commercial communications (spam) is an offence that has lately been taking on new forms and methods. In the Czech Republic the distribution of commercial communications is governed by Act No. 480/2004 Coll., on Certain Information Society Services. This is in principle a transposition of EU Directives 2000/31/EC on certain aspects of information society services, in particular electronic commerce, in the Internal Market, and 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. This means that the procedures against distribution of unsolicited commercial communications are the same in principle across Europe, with minor exceptions. In inspection practice new forms of distributing unsolicited commercial communications have been observed. The Czech Act No. 480/2004 Coll. prohibits the distribution of unsolicited commercial communications without the recipient's consent. Certain companies have decided to circumvent the law by hiring a company that distributes the commercial communications instead of them for a fee, as a kind of "front". For illustration we can describe the course and results of an inspection of the company below:

SCM Financial Insure Corporation s.r.o. (inspector Josef Vacula)
In the given case the unsolicited commercial communications were sent in the period from 25 November 2014 to 20 May 2016. They were sent from the e-mail addresses info@optimal-mailing.cz, obchod@bestmailing.cz and info@marketingmailing.cz. According to a statement from the whois database for these domain names, at the time the commercial communications were sent these domains were held by the company SCM Financial Insurce Corporation, s.r.o. From the Domain Name Server (DNS) records it is evident that specific IP addresses correspond

to these domains. These IP addresses are in the address range belonging to the company WEDOS Internet, a.s. WEDOS Internet, a.s. stated that the owner of that user account is the company SMC Financial Insurce Corporation, s.r.o. (hereinafter the "Inspected Entity"), Reg. No.: 28301064. Based on assessment of all the facts contained in the file documentation it is evident that the sender of the commercial communications in question was the above company.

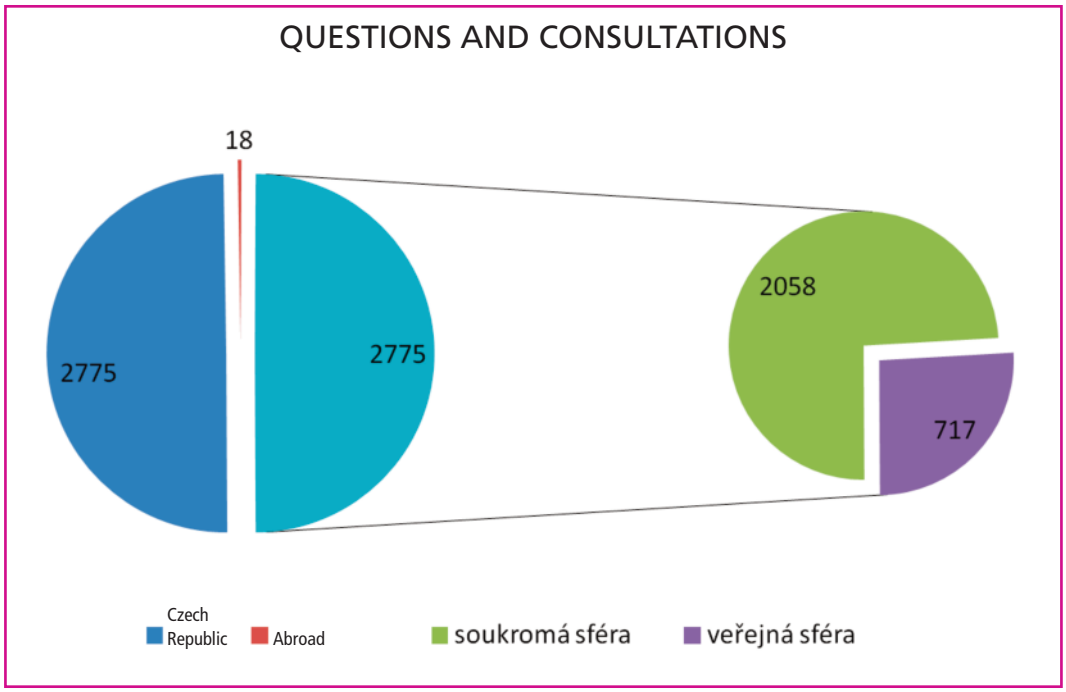
The inspector assessed whether the conditions for the sending of commercial communications listed under Article 7 of Act No. 480/2004 Coll. had been met, in particular the condition of only sending commercial communications following prior consent from the addressees. In the Notification of Commencement of Inspection, Notification of Expansion of Inspection and Notification of Expansion of Inspection II, the Inspected Entity was called upon to corroborate that the addressees from the e-mail addresses to which the commercial communications had been sent are their customers or to corroborate the consent of the individual addressees with being sent the commercial communications in question. Consent means a free, clear and conscious expression of will made by the addressee to the sender allowing the latter to make use of their electronic contact details to send commercial communications. It must be apparent from the consent who is providing it, to whom and for what purpose. Consent must be given in advance (before the commercial communications are sent) and must be demonstrable. In the case of commercial communications it is not necessary to evidence for what period consent is given as there must be the option to refuse this consent in each communication sent. Act No. 480/2004 Coll. does not lay down an obligatory form (such as written form) for consent to the sending of commercial communications. In the case of a conflict where the addressee of a commercial communication claims it was sent to them without their consent, the burden of proof lies with the sender. In such a case the sender is obliged to prove that the addressee agreed to the sending of a commercial communication and that the consent met all the above requirements. This means that the sender of a commercial communication must provide proof of consent from the addressee. Consent to the sending of a commercial communication must be acquired in advance (unless it is an existing customer) and must apply to a specific sender. The Inspected Entity however did not react to the Notification of Commencement of an Investigation, nor to the two expansions of the inspection nor to the requests that were sent to it. Based on the inspection findings, especially as concerns the domains from which the commercial communications were sent and the consistent claims of the complainants (who stated that they had not provided consent to the sending of commercial communications and are not its customers or registered users), and on the basis of the fact that the inspected Entity did not produce proof that the commercial communications were sent to the e-mail addresses in question with prior consent from the addressees or that the addressees were its customers, the inspectors considered it proven that the Inspected Entity, by sending commercial communications from the addresses info@optimalmailing.cz, obchod@bestmailing.cz and info@marketingmailing.cz concerning the offer of a database containing 400 000 e-mail addresses for natural persons from the whole Czech Republic, violated the obligations laid down under Article 7(1) and (2) of Act No. 480/2004 Coll., i.e. distributing commercial communications by electronic means only under the conditions laid down by this act, meaning only to users who have given prior consent.

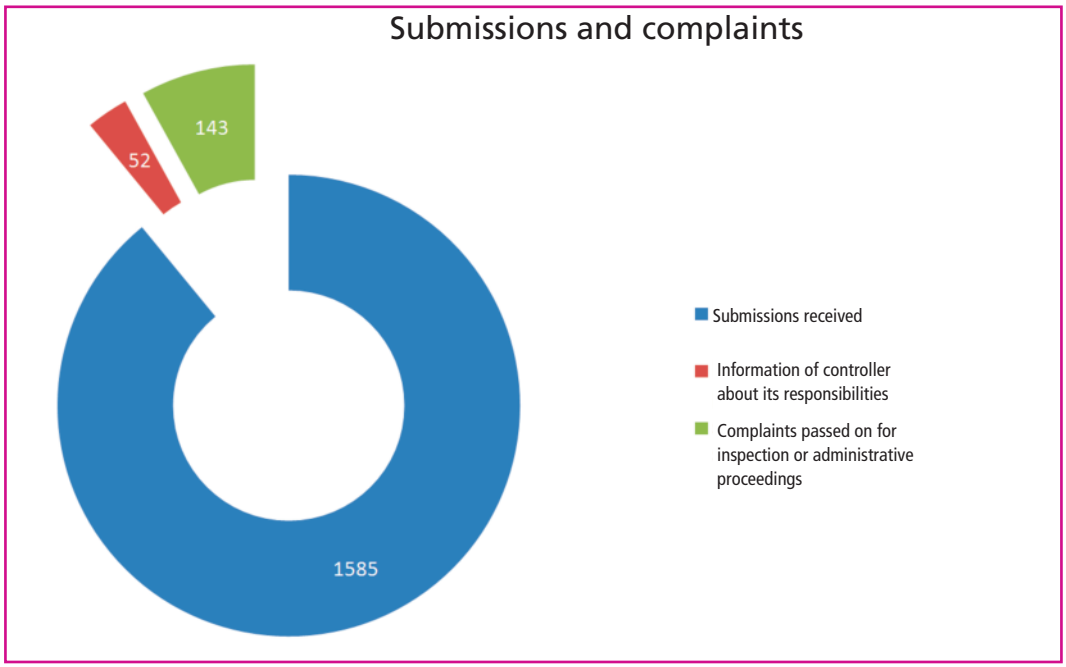
No objections were submitted by the Inspected Entity against the inspection report. It must be stated on this matter that the company was also fined for failure to cooperate (not reacting

to the Notification of Commencement of Inspection, the expansions of the inspection or the requests) pursuant to Article 16(1) of the Inspection Code in the amount of CZK 100 000.

These inspection proceedings were followed up by administrative proceedings, which were launched with the proceedings participant with a Notification in which the proceedings participant was called upon to make a statement on the further complaints that the Office received after the conducted inspection. It must be mentioned that even over the course of the whole administrative proceedings, commercial communications were constantly being sent out and complaints were being submitted about these unsolicited messages. During the administrative proceedings the participant was called on to make a statement on the sent messages a total of three times. It did not react to a single one of these requests, even though all the notifications were duly delivered by data mailbox. In light of the fact that even during the administrative proceedings the participant did not bear out the burden of proof, consisting of the fact that consent was given to the commercial communications being sent, the administrative authority considered it proven that the participant violated the obligations laid down under Article 11(1) a) with its actions, having repeatedly distributed commercial communications without the consent of the addressees. In determining the amount of the penalty, a fact increasing the gravity of the participant's behaviour in terms of the intensity of the administrative offence was that the sending of unsolicited commercial communications had taken place over a fairly long period of time, as well as the sheer amount of addressees of commercial communications. The administrative authority considers it an aggravating factor that the commercial communications were sent repeatedly to individual addressees and in five cases the commercial communications were even sent after explicit and demonstrable rejection of further commercial communications. It must also be considered an aggravating circumstance that multiple e-mail addresses were used to send the unsolicited commercial communications, which for the addressees meant greater trouble in blocking the sender addresses. Another aggravating circumstance that the administrative authority took into account in setting the amount of the penalty was the fact that the sending of commercial communications is part of the participant's business activity and all the more then should it have complied with the applicable legislation. Following an overall assessment of all circumstances the administrative authority issued a fine of CZK 300 000. The decision entered into legal force and on 16 September 2016 became enforceable. The penalty has not yet been paid, thus the Office forwarded the documents for enforcing the fine to the City of Prague Customs Authority.

Other Supervisory Activities





COMPLAINTS HANDLING AND CONSULTATIONS

Over the course of the year, a change in the legal treatment of certain laws concerning the processing of personal data came into effect, which was significantly reflected in the spectrum of received questions as well as in the method of assessing and evaluating the received complaints and submissions to the Public Relations Department, which as part of the Office's jurisdiction in accordance with Article 29(1)(c) and (h) of Act No. 101/2000 Coll. evaluates and determines the procedures for received complaints and submissions and provides written, telephone and personal consultations to data controllers and subjects as well as other involved parties.

First of all, we can mention the amendment to Act No. 634/1992 Coll., on Consumer Protection, which in the provisions of Article 20z institutionalises an information database on the credit and reliability of a consumer. This is a completely new legal treatment of "debtor registers", which were previously de facto unregulated (aside from the "Bank Register" under Article 38a of Act No. 21/1992 Coll., on Banks), which can now process personal data without the subject's consent for the purpose of protecting the rights and legitimate interests of retailers and consumers while at the same time observing the conditions and obligations defined by the Consumer Protection Act. The role of the Public Relations Department in this regard was primarily educational, informing the inquirers and complainants about this new legislation. This new legal treatment was also taken into account in dealing with complaints and consultations.

Another legal regulation that influenced consultation and complaint activities was Act No. 112/2016 Coll., on Registration of Sales, in connection with which the Office noted increased dissatisfaction from self-employed natural persons with their birth numbers being made accessible as a result of this data being listed as part of the tax identification number on the receipt. According to the provisions of Article 20(1)(b) of Act No. 112/2016 Coll., the taxpayer is obliged to list their tax identification number on the receipt issued to the person from whom the registered sale comes, i.e. every customer, who can then keep it as a document. The structure of a tax identification number based on birth number is laid down in Article 130(3) of Act No. 280/2009 Coll., the Tax Code.

Another legal regulation that influenced consultation activity in particular was Act No. 340/2015 Coll., on Special Conditions for the Effectiveness of Certain Contracts, Publication of Such Contracts and the Contract Register (the Contract Register Act). The subject of consultations associated with this law was largely the scope of personal data published to fulfil the obligation to publish the documents stipulated by the Contract Register Act.

The activity of the Public Relations Department under the consultation and complaints agenda was not however influenced solely by changes in the legislation, but also by adjustments to the Office's opinions expressed in the form of its position statements.

From the start of 2016, in association with the issuing of Office Position No. 1/2016 Placement of Camera Systems in Residential Buildings, the change in the Office's approach to the issue of camera recordings in apartment buildings was explained. This change aimed to allow

the use of such recordings for the legitimate purpose of protecting life, health and property while also thoroughly upholding the obligations arising from Act No. 101/2000 Coll. so that the recordings made cannot be misused to systematically monitor people, especially the residents of the building where the camera was installed. This change of position also influenced the assessment of tips and complaints about camera systems in residential buildings.

The issue of cameras in apartment buildings however only makes up a part of the total number of questions and complaints on camera systems. Other areas are camera systems in public spaces, in vehicles and last but not least also in workplaces, where however labour inspection authorities can take jurisdiction with regard to Act No. 262/2006 Coll., the Labour Code.

The thin line between the right to information and the right to privacy also comes into play in the complaints and consultations where the Office has to deal with the relationship between the Personal Data Protection Act and the Free Access to Information Act when providing information on natural persons by obligated entities pursuant to the Free Access to Information Act and the possibility of further handling of personal data acquired by the applicant in the position of a recipient of personal data. The complaints agenda frequently faces submissions on the publishing of address details for information applicants, which the Public Relations Department generally dealt with, especially in the case of e.g. a small municipality with insufficient legal awareness and the disclosure was not great, by informing the obligated entity that it cannot publish the applicant's identification information, and in the vast majority of cases the situation was quickly and efficiently rectified to the complainant's satisfaction.

This approach corresponds to the option that has been in the organisational regulations since 1 January 2016, which allows the Public Relations Department to inform the controller of its legal obligations in appropriate cases. The Public Relations Department made use of this approach in the case of minor infringements on Act No. 101/2000 Coll. or slight ignorance on the part of the controller. Using informative letters, dozens of cases were quickly and efficiently rectified to the benefit of the data subjects without the need for formal punishment in administrative proceedings or starting an inspection process.

The Public Relations Department endeavoured to cater to the trend of a computerising state administration by updating and adding to the answers to frequently asked questions, which form a separate section on the Office's website and allow quick information to be provided to site visitors, removing the need to send in an inquiry in some cases. At the same time a set of instructions for solving problems with personal data on the internet was issued and articles on current topics were published by the Public Relations Department to raise the informedness of the public.

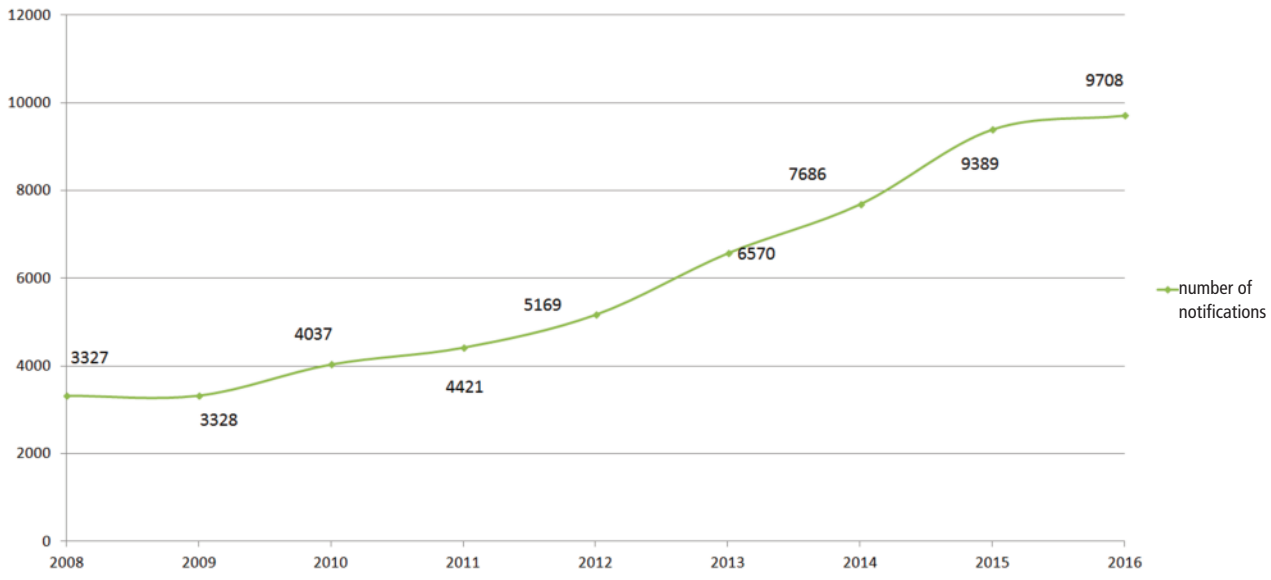
The topics of dozens of personal consultations provided at the Office's building to personal data controllers from among the ranks of public administration and private entities included the processing of personal data of participants in admissions proceedings at universities, the possibility of using cloud services to store sensitive health data, the processing of personal data as part of the activities of a political party or movement, records of authorised access to the Register for Restricted Medicines, the plan to create a "Robinson list" in order to prevent annoying calls by participants in electronic communication services, the use of GPS to optimise the routes of postal carriers, the project of an employment card for foreigners, electronic processing of passengers on mass transit, and transmission of personal data to third countries in connection with bank activities.

The publicly appreciated personal consultations, provided at the Office by Public Relations Department employees immediate upon arrival, primarily concerned the operation of camera systems in public and in residential buildings and the possibility of protecting one's own property with a camera system, as well as hundreds of diverse cases the issue of personal data processing comes up in in life.

REGISTRATION

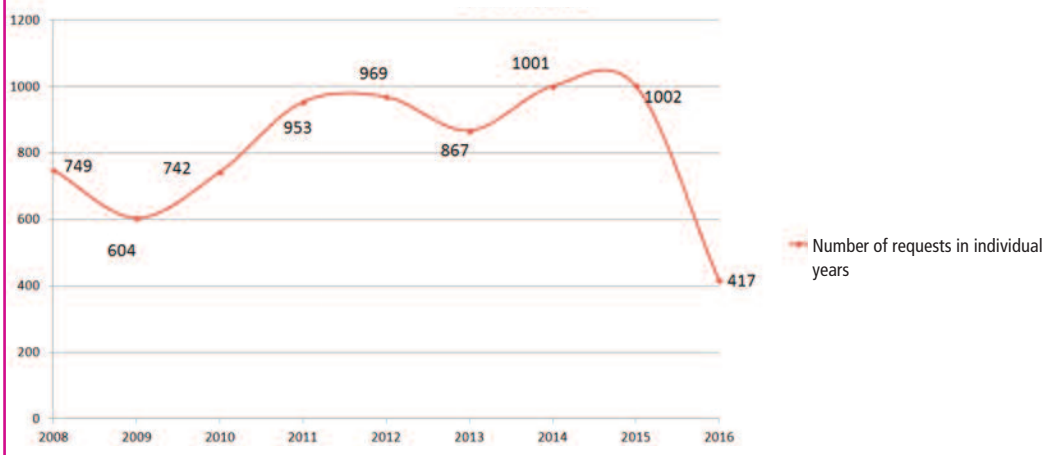
In 2016 the trend of previous years continued whereby the number of notifications on personal data processing has grown, in some years by as much as tens of percentage points a year. Over the last twenty years the number of notifications received has grown by 292%.

Number of notifications in 2008–2016



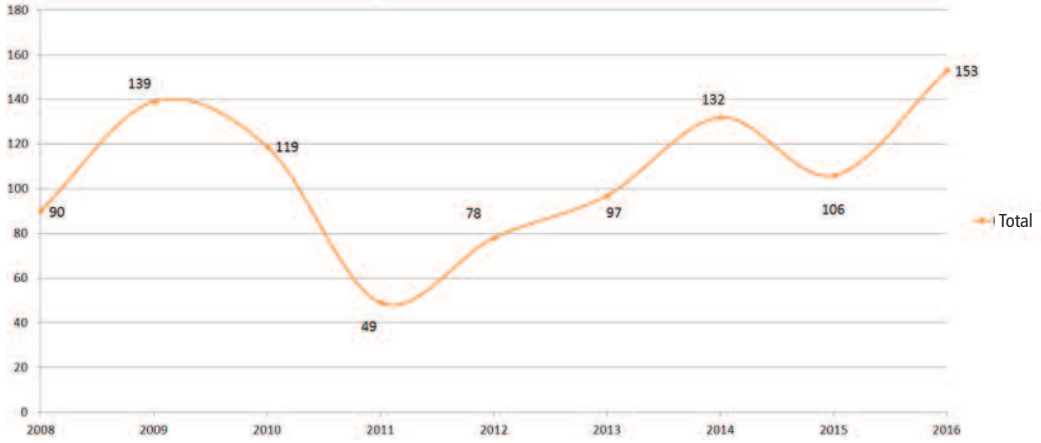
If a notification does not contain all the requirements necessary to assess the processing of personal data, the controller is sent a request to fill in the required information. In 2016 the Office launched a total of 417 registration proceedings under Article 16(4) of the Act on Personal Data Protection. In terms of the number of commenced registration proceedings, there was a significant drop this year, caused primarily by a modification to the part of the registration form concerning camera systems – see below. Another factor was the gradual downplay of the importance of registration in light of the new General Data Protection Regulation which takes effect in May 2018 which no longer counts on a general notification requirement. While in previous years the number of commenced registration proceedings accounted for around 17% of the total amount of notifications received, this year it was only 4.3%.

Number of commenced registration proccedings in the years 2008–2016



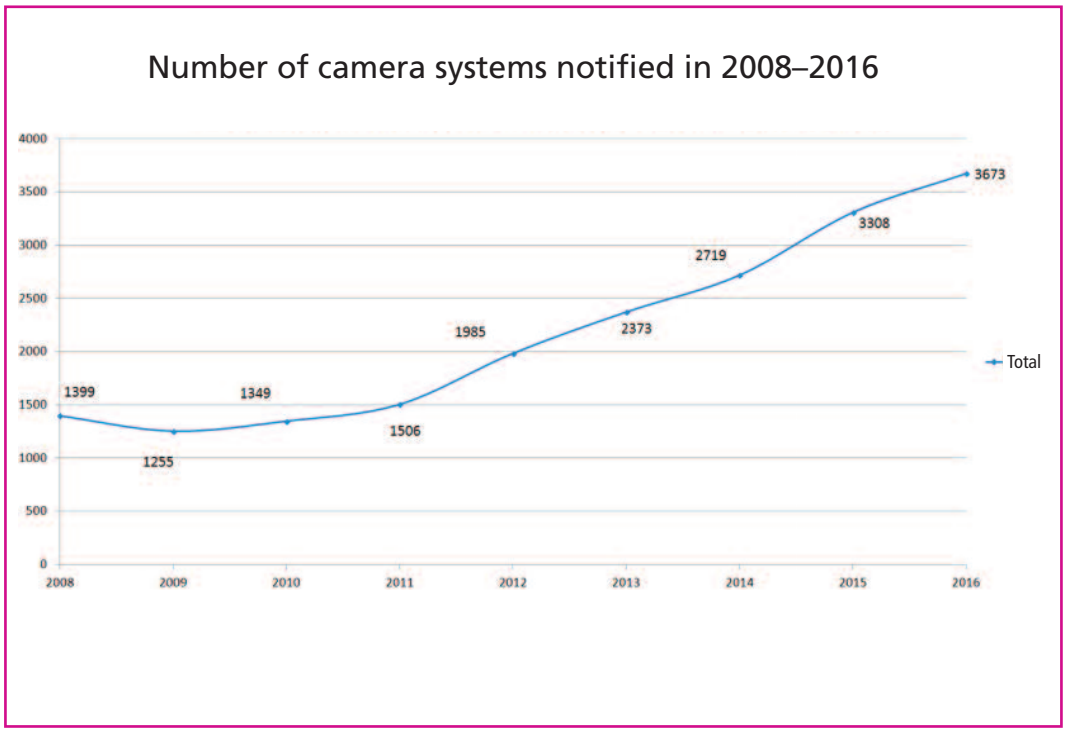
Aside from assessing received registration notifications, the Office also issues decisions on cancellation of registration pursuant to Article 17a (2) of Act No. 101/2000 Coll. This year a total of 153 cases of processing were cancelled at the request of the controller, most frequently due to the dissolution or merger of the company, cessation of business activity, or termination of personal data processing. The graph below shows that in this case as well the Office recorded an increase in the number of requests of controllers to cancel registration.

Cancellation of registration under Article 17(2) by request of controller in 2008–2016



According to Article 19 of Act No. 101/2000 Coll., a controller recorded in the processing register has the obligation to tell the Office after ending its activity what it did with the personal data. As this obligation is frequently not upheld by controllers, the Office moved to remove the files of no-longer-existing entities from the public register on the basis of the Register of Persons and Register of Inhabitants, thereby "cleansing" the public processing register of thousands of cases of processing that is no longer taking place because the original notifier/controller has dissolved or, in the case of natural persons, diseased.

The most frequent type of processing (around 38% of the total number of notifications received) that turned up this year was, much like in past years, processing by camera system. As the graph below shows, here too the number of notifications has a rising tendency. A total of 3673 entities who have submitted a notification of personal data processing by camera system are recorded in the register of personal data processing, Since 2008 such notifications regularly comprise around one third of all received notifications and processing cases.



The part of the notification form for personal data processing concerning camera systems was also modified in 2016. A system using check boxes was chosen, with potentially added text description. This allows controllers to easily describe the characteristics of the camera system (placement, regime, retention period, informedness of data subjects, measures adopted to protect personal data) simply by choosing from the options offered. The options were set up on the basis of long-term monitoring of the most frequently notified parameters for camera systems. In the case of describing the technical and organisational measures, the processing of personal data by camera systems seems so specific that it was separated into a separate point. If the controller chooses uncommon or problematic characteristics for the camera system, it must add a comment where it describes and in certain cases also justifies why they were chosen. This approach should guide the controller so as to choose trouble-free solutions in

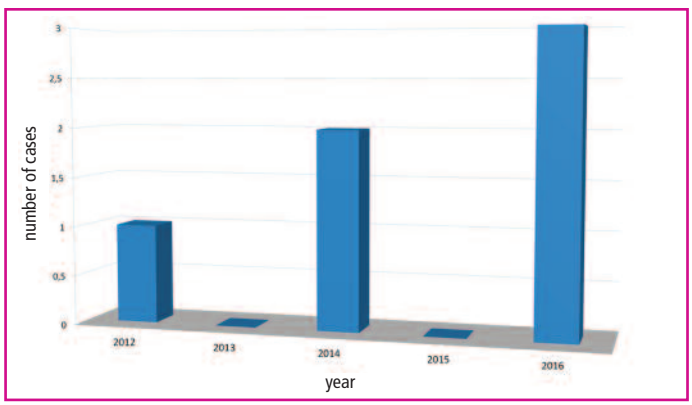
designing the camera system in terms of personal data protection. This then brings the Office less administration associated with accepting notifications on personal data processing (fewer questions, fewer requests for additional information).

This year there was an increase in notifications concerning the placement of camera systems in public transport vehicles in certain major cities. The purpose of installing camera systems in public transport vehicles, or cameras capturing the area in front of a vehicle, is protection of property against damage and vandalism, increased passenger safety and prevention, using the recording as evidence of a crime or damage, or to clarify the causes and resolution of emergencies, and to protect employees against attacks. This solution is possible under certain conditions, which include restrictions on deployment (only on critical connections or only on connections with the city limits), increased risk (there has been an increase in crime or damaging of property), sufficient security (in particular where access to camera records is only possible with the physical presence of the Police of the Czech Republic) and regular review of the cameras along with adjustments to the number of cameras based on the results of deployment.

In connection with the development of information technology, special methods of personal data processing conducted via these new technologies are appearing ever more frequently. In particular this applies to the increasingly frequent use of biometric systems that are used as part of the security measures for checking persons entering buildings, or certain workplaces, the checking of access rights when working with a computer, attendance systems, and ever more frequently in advertising and marketing as well. In 2016 the Office received a notification on the processing of personal data of persons entering schools based on the processing of fingerprint characteristics (using templates) in order to protect students at the schools. In light of the fact that it was evident from the notification that this is already actively underway, the signal was given to launch an inspection.

Breach of personal data security in electronic communications

Once again this year there was no increase in the number of notifications, as can be seen from the graph. After five years of experience it can be stated that obligated entities are highly sporadic in fulfilling this legal obligation. The situation is similar in the majority of other EU member states as well. One of the main reasons for the lack of interest by controllers in reporting such cases can be seen in notifiers' fear of possible penalties if they admit that the security of personal data at their company was breached. In contrast, failure to report an incident is not punishable. In this regard the new General Data Protection Regulation will bring about a change, as it envisages a fine of up to EUR 10 million for fail to report breach of personal data.



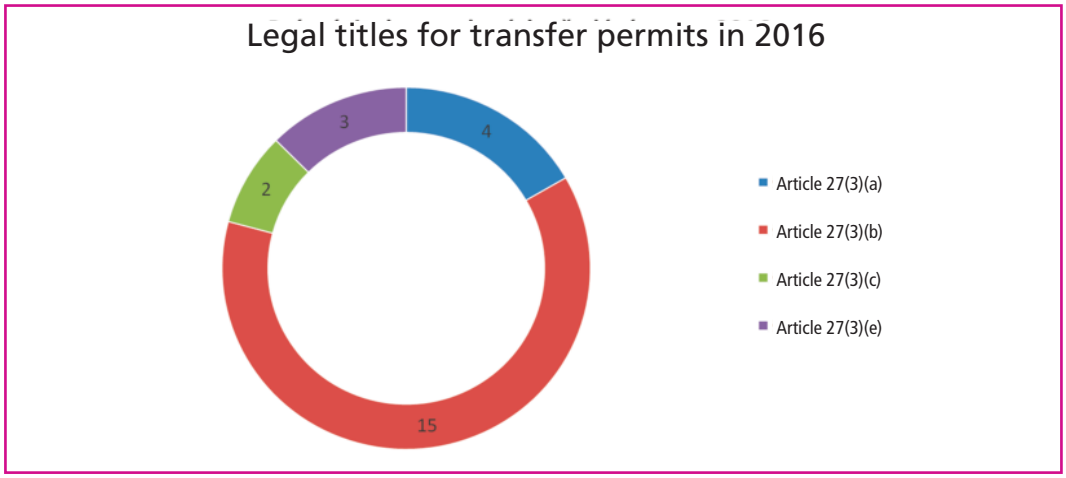
In 2016, three such cases were reported. The most significant of them concerned the theft of customer personal data (in the hundreds of thousands of people) from a telecommunication company by its employee. The stolen data was offered for purchase to another company by the employee. In light of the problematic set-up of the technical and organisational measures at the affected telecommunication company, it was fined CZK 3.6 million of the maximum possible rate of CZK 10 million.

Transfers of Personal Data Abroad

In 2016 the Office issued 24 permits for the transfer of personal data to third countries under Article 27(4) of Act No. 101/2000 Coll.

The most frequent legal title under which the Office issued the permits was Article 27(3)(b) of Act No. 101/2000 Coll. as the applicant created sufficient special guarantees of personal data protection in the third country, always through the approval of binding corporate rules (BCR). This took place in 15 cases.

Three times the legal title for the permit was Article 27(3)(e), i.e. the transfer of data necessary for negotiations on conclusion or amendment of a contract made at the initiative of the data subject, or for performance of a contract in which the data subject is a party. Four times the legal title was Article 27(3)(a), i.e. transfer of data with the consent of or based on an order from the data subject. In two cases the Office issued a permit for access to cadastre data based on the fulfilment of the conditions laid down under Article 27(3)(c) of Act No. 101/2000 Coll.



Thus the trend already familiar from previous years was confirmed whereby the responsible personal data controllers do not rely on consent from the data subjects, but deal with the transfer of data to third countries with an insufficient level of personal data protection by using instruments that ensure the transferred data adequate protection in the third country as well. Alongside the aforementioned binding corporate rules, these primarily include standard contractual clauses. When using standard contractual clauses, according to a decision of the European Commission it is not even necessary to ask the Office for a permit, as the transfer then takes place under the provisions of Article 27(2) of Act No. 101/2000 Coll. on the basis of a European Union decision.

Geographically speaking, transfer to multiple countries considerably prevailed over transfer to one single country, or rather transfer to a large number of branches in many countries, in which there is typically a group to which the Czech personal data controller also belongs as a branch of a multinational group, with this group ensuring protection of personal data shared within the group via the aforementioned binding corporate rules. Another model situation is travel agencies, which transfer clients' personal data to their partner organisations, which secure accommodation, transport and other tourism services in foreign tourist destinations.

Analysis of personal data flows to third countries as of 16 February 2016

To make it possible to acquire at least a general idea of the flow of personal data from the European Union to the United States and its significance in comparison with other countries, the Office conducted an analysis of data on transfers of personal data contained in the processing register. As part of the notification obligations under Article 16 of Act No. 101/2000 Coll., personal data controllers provide information on whether they intend to transfer data to third countries outside the European Union, and if so to which ones and whether they will use standard contractual clauses. The Office updated and elaborated on the analysis as of 16 February 2016. It turned out it was a unique analysis within the whole European Union, thus we consider it appropriate to make the results of this analysis public here.

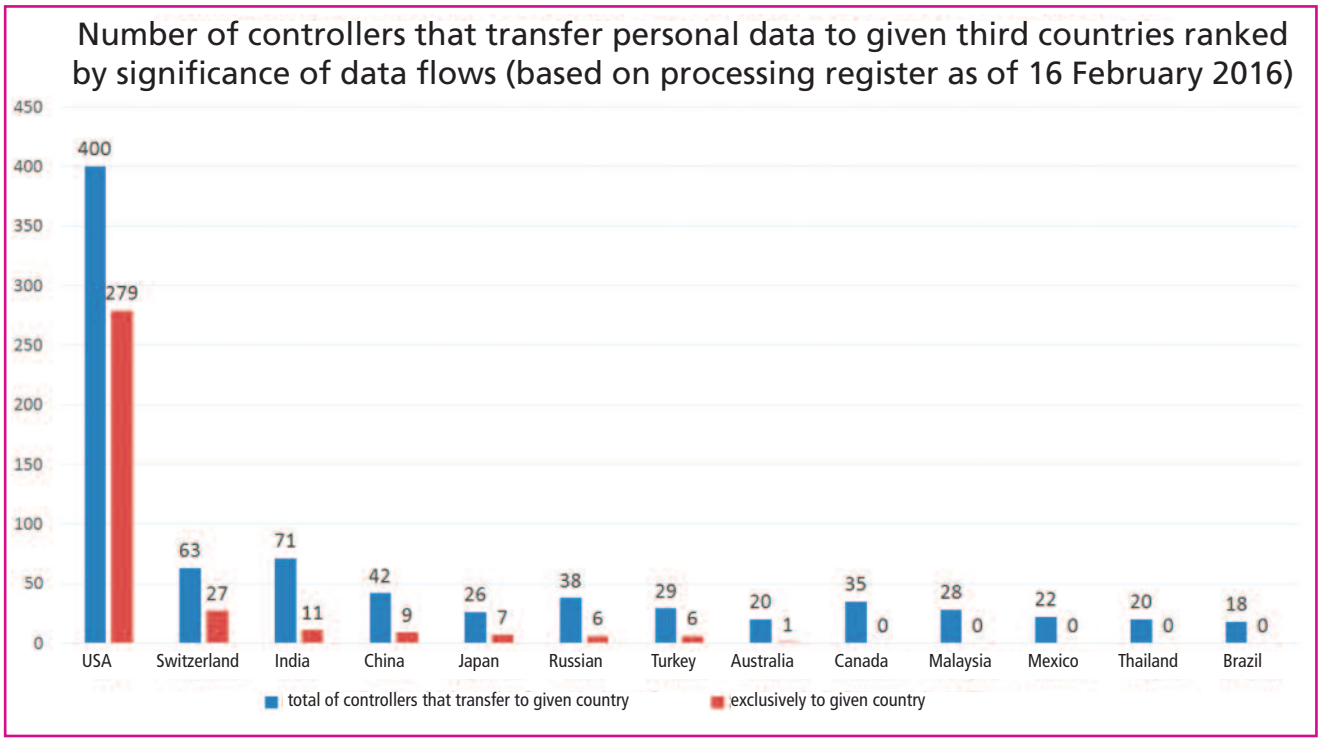
As of 16 February 2016, 1922 personal data controllers were found in the register who had stated that they were transferring personal data to third countries in any of their currently registered notifications as per Article 16 of Act No. 101/2000. A large number of these controllers filed their notifications in the first years after the Office was founded, when controllers did not have to report the specific third countries to which they intend to transfer personal data, nor use of standard contractual clauses. This is the main reason that the analysis provides only an indicative value in terms of absolute numbers, yet it does not lose its value in terms of comparing the number of transmissions to individual third countries.

The main result of the analysis is summarised in the table below of showing the third countries to which personal data are transferred most frequently. The total number of controllers transferring data to a third country is broken down in the table into the number of personal data controllers that transfer data exclusively to that third country and the number that transfer

personal data to that country and other third countries. It would appear that the number of controllers that transfer exclusively to the given country better reflects the significance of the given country as a real target country of data flow, where parent companies and major personal data processors are based. For this reason the graph based on the table orders the countries based on the importance of those third countries to which personal data are transferred.

	Number of controllers transferring personal data to third countries		
Third country	Total	Exclusively to that country	Also to other third countries
USA	400	279	121
India	71	11	60
Switzerland	63	27	36
China	42	9	33
Russia	38	6	32
Canada	35	0	35
Turkey	29	6	23
Malaysia	28	0	28
Japan	26	7	19
Mexico	22	0	22
Australia	20	1	19
Thailand	20	0	20
Brazil	18	0	18

Table: Third countries ranked by number of controllers that send personal data to the given third country. Source: Office´s register of notified processing operations as of 16 February 2016



It follows from the above table and graph that the United States of America are the completely dominant recipient of personal data flow transferred from the Czech Republic out of the European Union. The United States have six times the number of transferring controllers from the Czech Republic than the following India and Switzerland. In terms of the significance of data flows, the United States surpassed second-place Switzerland tenfold and each of the following group of third countries roughly thirtyfold in the order India, China, Japan, Russia, Turkey. It was also shown that aside from these seven countries, there is no other third country that plays a significant role as a receiver of personal data flows from the Czech Republic, neither the countries listed in the table Australia, Canada, Malaysia, Mexico, Thailand and Brazil, nor the ones that follow them in number of transferring controllers, which are Serbia (17), Egypt (15), the Philippines (14), Norway (14), Croatia up until it entered the EU (14), Argentina, South Africa (13), South Korea (12), etc.

The transfer of personal data to the United States of America was also evaluated from the perspective of the legal title of the transfer. It must be pointed out again that the data in the processing register cannot reflect the exact current state of the given issue, as the registration obligations under Article 16 of the act only indirectly relates to the obligations of a controller transferring personal data abroad under Article 27 of the act. Nevertheless it can be stated that a majority of the approximately 220 contacted controllers who according to their registered notifications were still transferring personal data to the United States of America in October 2015 based on the recipients' involvement in the Safe Harbour programme not only reacted to the change of situation and secured protection of transferred personal data in a different manner, but also reflected this fact in the processing register and made a change to its registered notifications in the above sense. The majority of controllers evidently made use of the institution of standard contractual clauses.

At the same time, in recent years the Office has most frequently issued permits based on submitted binding corporate rules (BCR) of the group in which the transfer of personal data to third countries is being realised in the regime of Article 27(3)(b) of Act No. 101/2000 Coll. The Office currently issues permits for a limited period, generally three years. As of 16 February 2016, the Office had 35 valid permits for the transfer of personal data to third countries based on BCR on record, of which 34 included the transfer of personal data to the United States of America (of that amount 10 exclusively to the USA and 24 to other countries as well).

An analysis of the flow of personal data to third countries made on the basis of data in the processing register as of 16 February 2016 showed that a majority of the approximately 220 contacted controllers took the Office's recommendation seriously and secured the transfer of personal data to the USA through standard contractual clauses or binding corporate rules. It was thus shown that it is essentially possible to replace the Commission's overturned Safe Harbour decision with existing alternative instruments when transferring personal data to the USA.

The analysis also demonstrated that the United States of America is by far the most important target country for personal data flow from the Czech Republic out of the European Union. This significance of the United States of America as a recipient of personal data from the Czech Republic can be explained through two fundamental factors. The first is the fact that many parent companies and headquarters of branches that act in the Czech Republic are based in the United States. The other is the fact that a majority of the major companies that provided information society services of various types, including cloud services, are based and manage

collected data in the United States of America. At the same time the level of use of US software platforms, social networks and cloud solutions in the Czech Republic and indeed the whole European Union, which is inextricably tied to personal data flowing to the USA, is so widespread that no other third country can even come close to the United States in this regard.

These reasons, including the political and economic overlap of the importance of transatlantic person data flows, have led the WP29 working group and the European Commission to the conclusion that it is necessary to adopt a new robust instrument for protecting personal data transferred to the USA as soon as possible to replace the existing Safe Harbour programme and ensure the renewal of trust of the EU population in adequate protection of personal data transferred to the United States of America.

SCHENGEN COOPERATION

The legal treatment of extensive European information systems, which include the Schengen Information System (SIS II), Visa Information System (VIS), Eurodac and the Customs Information System, place great emphasis on the area of personal data protection and active fulfilment of the associated obligations by supervisory authorities. In the Czech Republic this supervisory authority is the Office for Personal Data Protection. Aside from supervision and inspection associated with the meeting of the requirements for legal processing of personal data on the part of a controller and under the aforementioned systems, the Office also dealt with the creation of new information systems, in particular as regards the processing of personal data. An example is the EES system (Entry-Exit System) focused on processing the personal data of third party nationals with the right to a short-term stay within the European Union. Another system just being created is ETIAS, under which the personal data of persons from third countries with no visa obligation are processed. With regard to the large amount of personal and sensitive data being processed in these types of system, it is essential to ensure a corresponding level of protection for the rights of data subjects, as observation of the principles of personal data protection is a primary precondition for the transparent functioning of information systems under Schengen cooperation.

Activities of individual coordination groups in Schengen, visa and customs cooperation

The primary activity of coordination groups in 2016 was preparing the joint inspection models that will lead to harmonisation of inspection procedures of individual countries taking part in using the information systems.

Under the coordination group that watches over the legality of data processing in the Eurodac system, a single model of inspection questions for the national inspectorates in the Eurodac system was drawn up and approved. The goal of the shared form of inspections realised in the individual member states is to be output that allows comparison of the functioning and administration of the system in terms of personal data protection.

The coordination group for oversight over CIS (Customs Information System) is also preparing a common inspection format. The Czech Republic was designated to fulfil the role of rapporteur in these preparations. As part of this group's activities, a shared guide for applying

the access rights to data processed under CIS was drawn up, including forms for data subjects. This document will be made available in 2017 on the Office's website as well as on the website of the Customs Administration of the Czech Republic in the section European Union/CIS.

Current problems being dealt with under the coordination groups

The coordination group for the Eurodac system (Eurodac SCG) was currently dealing with the issue of a draft retooled regulation on the Eurodac system. The Commissioner for Migration, Home Affairs and Citizenship, Mr Dimitris Avramopoulos, was sent a letter on behalf of all the members of the coordination group in autumn of 2016 expressing concerns over the proposed changes. Particularly the proposed reduction of the age limit of persons whose fingerprints are taken – from fourteen to six years of age, the retention of applicant photographs in the central system with the aim of future use of face-recognition software based on biometric identifiers, and the extension of the time limit for keeping personal data are fundamental changes that must be brought in line with the basic principles of personal data protection.

The coordination group for the Visa Information System (VIS SCG), as part of the changes reacting to the adoption of a new Schengen evaluation mechanism (Council Regulation No 1053/2013), is preparing a separate chapter dedicated to the Visa Information System, which will now be included in a document for the Schengen Information System coordination group with the aim of updating the joint recommendations for Schengen evaluation.

Furthermore, the aforementioned coordination group dealt with implementation of Article 41 of Regulation No 767/2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, which obliges national supervisory authorities to conduct an audit of data processing in the national VIS at least once every four years. Through a survey it was found whether an audit was conducted, in what manner and what recommendations for the system administrator came out of it.

In the past year, the coordination group for the Customs Information System (CIS) prepared, among other things, a single document governing the general rules for personal data processing in CIS. As part of a brochure, the rules for bringing the rights of data subjects to bear in individual member states including the Czech Republic are clearly defined. This document was modified with regard to the national legal treatment and in spring of 2017 it will be published on the Office's website as information for the public in the section EU Information Systems (Schengen).

Numbers of submissions, complaints and questions and how they were dealt with

During the past year the Office received a total of 10 submissions concerning the processing of personal data in SIS II. All cases involved realisation of the data subject's right to access to data in SIS II, either through the right to information or the right to erasure of personal data from the system. The main role of the Office is to review the approach of the personal data controller at the national level, which is the Police of the Czech Republic, with facts attesting to the violation of the data subject's rights only being found in one case.

The Office also received 17 submissions in which the petitioners inquired about the visa policy of the Czech Republic or the course of processing of their visa requests. in light of the fact that this matter does not fall under the Office's legally defined jurisdiction, the petitioners were referred to the Ministry of Foreign Affairs, which is responsible for the given issue. In connection with this the Office clarified its jurisdiction defined by Act No. 101/2000 Coll., as well as by the EU legislation.

6 Analytical Activities

CREATION OF ANALYTICS UNIT

Mid-way through 2016 the Office established an analytics unit, which gradually began to fulfil its function and integrate into the Office's activities. The Office thus joined the ranks of state authorities that place an emphasis on dealing with complicated and complex issues under its jurisdiction systematically. In general, analysis indicates intellectual activity that is used for problem-solving or coming to a conclusion on solution possibilities. Legal analysis can serve to help find a proper or just solution to a problem, identify various possible solutions or find the need to change the legislation. The starting point for doing so is generally the current legal treatment, case law and acts of application of the law; also usually taken into a account is EU law, and potentially the legal treatment in other EU member states. The Office's analytics unit also uses these methods.

In the second half of last year, the newly created unit devoted attention both to general issues of personal data protection as well as personal data protection in relation to the individual sub-areas of the legislation. This included the issue of personal data protection in the land register, the relationship between the Civil Service Act and the obligation of confidentiality, the position of a data protection officer under the General Data Protection Regulation and the setting of principles that should be taken into account when issuing e-tickets (smart cards). In connection with a statement on constitutional complaints, the Office drew up an analysis of disclosed civil servant salaries and pointed out the specifics of personal data protection in the archives of post-communist countries, which the EU also counts on. Below are some of the major conclusions of selected analyses.

1. Personal data protection in the land register

The Office devoted increased attention to protection of personal data in the land register. Specifically it addressed whether this protection is sufficient, whether there were cases where property rights of individual citizens were damaged (theft or attempted theft of real estate) as a result of fraudulent actions

by persons who abused the personal data of the owners obtained from the land register. In this context both the protection of personal data and the principle of publicity of the land register have significance. The relationship of these should be balanced. On the one hand, information about real estate should be accessible to all entities who need to know the owner of a property for justified reasons; on the other hand this information should only be accessible to third parties or the public to the extent necessary and beyond this should not be provided (principle of data minimisation).

In conclusion we can summarise the changes that could potentially be desirable in terms of the land register from the perspective of personal data protection:

– paper documents should only be provided to those entities that have a legitimate interest (this would mean a change to the legislation)
– a data subject should receive information on the processing of its personal data provided to the recipient of the data (can be done based on the existing legislation)
– personal data in paper documents should be anonymised
– measures should be adopted to make paid services for monitoring property superfluous

2. **Disclosure of civil servant salaries (statement on constitutional complaint file No. IV. ÚS 1378/16)**

The subject of the constitutional complaint was the objection of the complainants to the provision of information on their salaries based on Act No. 106/1999 Coll., on Free Access to Information, and a proposal to strike down Article 8b thereof. The complainants inferred that the provision of information on their salaries is a serious breach of their privacy, with which they do not agree. The Constitutional Court requested that the Office make a statement on the proposal as the central administrative authority for personal data protection. Some of its conclusions on the issue in question are contained in the following text:

- The legal treatment of the issue of publishing salaries at public administration bodies is marked by a high level of sensitivity from the perspective of the subjects about whom information is provided. It is the subject of expert discussions and accompanied by a good deal of media interest. in essence it is a case of a clash between the right to information and the right to personal data protection. From the perspective of comparative law it is true in general that the relationship between the two rights, in terms of which one to give priority to, can be assessed in different ways and there are multiple possible solutions. Aside from taking on a categorical opinion on the question of whether to disclose employee salaries or not, there are also compromise solutions such as setting a cut-off over which salaries are disclosed, or publishing income based on the type of function held or pay component. Nevertheless it can be stated that the prevailing approach in Europe is not to publish the salaries of specific persons, though in the medium term the number of countries that have given priority to the right to information on salaries as regards management employees is on the rise. [1]

[1] Parlamentary Institute: Public access to salaries of top civil servants in selected countries. Information document No. 5.3,24. December 2011.

- In terms of the Czech Republic, access to disclosure of salaries has gradually developed, both in terms of the legal treatment and the case law, particularly of the Supreme Administrative Court (SAC), which has gradually found reasons for priority both for the right to protection of information and the right to privacy. With the adoption of SAC extended chamber decision No. 8 As 55/2012 of 22 October 2014, the contradictory case law was harmonised with the chamber taking a relatively radical position on the disclosure of civil servant salaries. The extended chamber came to the conclusion that the salary, wage or other consideration paid out of public funds are in principle always, with a few exceptions, income from public funds within the meaning of Article 8b of Act No. 106/1999 Coll. For this reason they should be made public in the majority of cases. The decision formulated two groups of exceptions from the obligation to publish the amount of salaries, specifically if the persons take part in activity indirectly and insignificantly and also if no doubts arise as to whether the funds are being spent economically.

- In assessing this it is primarily appropriate to accept that the case of provision of information on civil servant salaries or remuneration is one of a conflict between information obligations and the right to privacy. In such cases the Constitutional Court generally rules that it is necessary to carefully weigh all the circumstances as to whether one basic right is not being given undue priority over the other, while also examining the sense and essence of fundamental rights (Article 4(4) of the Charter). For this assessment a **proportionality test** is used (assessing the necessity, appropriateness and proportionality in the narrow sense).

In conclusion the Office proposed pro *futuro* that the **starting point for assessing whether it is necessary to provide personal data should be the purpose of the right to free access to information, which is the *proper, efficient and economic use of public funds***. This criterion is also used in the ECJ case law. This objective could be achieved in many cases by detailed publishing of relevant information in a prescribed structure without the personal data of employees such as year of birth or address having to be published.

3. **Access to data in archives (statement on constitutional complaint Pl. ÚS 3/14)**

At the request of the Constitutional Court, the Office provided a position on a constitutional complaint launched at the proposal of the Supreme Court of the Czech Republic, in which it was requested that Article 37(11) of Act No. 499/2004 Coll., on Archiving and Records Management and Amending Certain Acts (Article 37(6) in the wording in force up until 30 June 2009) be declared unconstitutional. According to this provision, an exemption applies to archival materials created before 1 January 1990 from the activities of military tribunals and all levels of public prosecution and security services as per the Act on the Institute for the Study of Totalitarian Regimes and on the Security Services Archive, as well as of special people's courts, the State Court, the National Court and social organisations and political parties associated under the National Front, as well as the activities of other entities cited in the law, consisting of the fact that no written consent from the person to whom the archival material applies is required for the use thereof.

- In the given context, the Office adopted the position that from the perspective of personal data protection the process of disclosing documents in relation to the past is personal data processing with a specific purpose, which is a significant societal interest in coming to terms with the past. In this process, specific information on various persons, situations and decision-making processes in a totalitarian regime plays a fundamental role. Many personal data were collected and processed by the repressive authorities of a totalitarian state using methods incompatible with the principles of the rule of law. These have a specific informative value and are essential to understanding the past. Their common denominator is documenting the nature, function and methods used by a totalitarian regime.

4. Personal data protection in using electronic cards in public transport

Legal issues associated with the protection of privacy and personal data are playing an increasingly significant role in the development of systems of integrated/interoperable smart tickets. With smart cards being used in more and more places and increasing amounts of data being stored on them, personal data are potentially becoming available to a greater number of persons and organisations. Business entities that manage these cards can often monitor the travel behaviour of individual service users. This information can be used to improve transport routes and timetables, but in general they can also be used without the customer's express consent for marketing or other purposes. With an eye to this, system owners are required to fulfil a large number of technical and procedural measures to protect privacy and customer personal data. Aside from that it seems useful to observe certain general principles that certain international organisations or working groups thereof that deal with this issue have come up with (e.g. the Article 29 Working Party, or the special group for e-tickets in urban public transport set up under it). In terms of assessing impact on personal data protection, in general it is recommended that transport company information systems be designed and implemented so as to take into account the right of customers to protection of their personal data by observing principles such as anonymity, transparency, data minimisation and retention period.

Legislative Activities

GENERAL

In 2016 the Office continued with its policy of transparency and published important positions on draft legislation and government conceptual documents on its website; it also pointed out the most important of these in the news section of the home page – on the National Health Information System, support for sports, the 3rd conceptual amendment to the new Labour Code, the population register and birth numbers, DNA, municipalities sending special birthday wishes, the Czech Trade Inspection Authority and the criminal liability of legal entities.

The total of 20 pieces published on draft legislation can be summarised as follows:

- The trend of shifting from paper to electronic documents is continuing. It is however complicated by the fact that many electronic documents are not structured texts (machine-readable is the EU technical term) but simple pictures. In 2016 the eIDAS Regulation went into force in 2016, as did its implementing act (No. 297/2016 Coll. on Trust Services for Electronic Transactions).
- A rather unfortunate trend is that an increasing number of supervisory authorities want to take on the powers of the police, in particular the possibility of discreet surveillance or establishing a secret agent, without court permission. The Office believes that supervisory authorities should operate openly, expertly dealing in particular with systematic (conceptual) problems, and leave the fight against crime to the Police of the Czech Republic.
- At several ministries the situation remains whereby the Office is left out as a mandatory consulting site. The Office evaluates such errors and asks the ministries in question to improve cooperation so that Article 36(4) of the already adopted but not yet in effect GDPR can be fulfilled: "*Member States shall consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by a national parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.*"

Point 4 of Government Resolution No. 820 of 14 November 2012 introduced effective 1 January 2013 an evaluation of the current state of planned legislation and bills for all national legal regulations (acts, government orders and decrees) and the impact of the proposed solution in relation to the protection of privacy and personal data (DPIA). Constant pointing out of the purpose and requirements of DPIA or repeated explanation of DPIA has already had a positive effect for some supreme administrative authorities, e.g. in general at the **State Authority for Nuclear Safety** or specifically for the draft amendment to the **Act on Building Savings** from the Ministry of Finance.

DPIA examples

The submitter sometimes brushes off DPIA with a formal statement, because it factually improperly determines the scope of the affected personal data processing, even for bills that establish extensive processing of personal data. For example, in the draft amendment of the **new Criminal Code** for fighting the financing and support of terrorism, racism, xenophobia and other intolerance, the Ministry of Justice stated that "*in this area the bill does not change the existing treatment in any way and no impact on the issue of privacy and personal data protection is expected*". in fact the criminal offence of incitement to hatred or violence toward a group of persons or restriction of their rights and freedoms now defined under Article 356(1) will have an impact on protection of sensitive data along with criminal repression: this applies to any handling of such data, regardless of whether they are factually correct. Criminal law protection should now be explicitly provided to the individual as well and the list of sensitive data that are protected from being handled under the purposes defined by the definition of the crime itself has been expanded and refined.

In 2016 the problematic Article 20z of the **Consumer Protection Act** took effect, establishing an information database on the solvency and credit record of a consumer. This is a confirmation that the neglecting of personal data protection and DPIA is a problem of initiated (by MP, Senator or Region) bills in general.

For seven draft **international agreements** that were submitted for assessment at various phases of negotiation, e.g. the Council of Europe Convention on the Manipulation of Sport Competitions, full respect for the principles of personal data protection was found and only in one case was a minor comment raised.

Public order

Of particular significance was a bill unclearly labelled as "*amending the Act on the Police of the Czech Republic and the Act on the General Inspection of Security Forces*", that is the draft Act on (a national database of) **DNA**. The bill merely legalises the current state, thus it unilaterally gives priority to the security perspective over protection of privacy. The Office cannot agree to the enormous scope of the national DNA database (all intentional crimes aside from four offences instead of those where there is a biological trace, i.e. for violent, property and moral crimes), the enormous retention period (up to 80 years from the committing of the crime) and the persistent fundamental factual errors ("future identification") in the Police Act.

National security

For the draft amendment to the **Act on Military Intelligence**, the Office requested that, among other things, the draft be added to and expanded to include a provision enshrining

supervision over the processing of personal data by Czech intelligence services. The reason was that the bill expands primary access to operating and location data produced from the operation of networks and electronic communication services in an area that is explicitly excluded from the supervisory jurisdiction of the Office. The Ministry of National Defence did not comply with this request. At the same time the Office of the Government proposed a reform of oversight over intelligence services in the draft amendment to the **Act on Intelligence Services of the Czech Republic**. It forgot to send the bill to the Office for a statement however.

The Office took part in transposing Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the **NIS Directive**). No problems relating to personal data protection were identified. The key thing in practice will be figuring out coordination of the notification of cases where personal data security has been breached pursuant to Article 33 of the GDPR, reporting personal data security breaches under Article 3(3) of the Privacy and Electronic Communications Directive and reporting of incidents with a serious impact on the continuity of basic services pursuant to Article 14(3) of the NIS Directive.

Handling of Complaints under Article 175 of the Code of Administrative Procedure

The Office had to deal with complaints under Article 175 of Act No. 500/2004 Coll. in 2016 as well, handling a total of 33. 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 Article 175 of Act No. 500/2004 Coll. Of the total number of such complaints, 2 were found to be justified and 11 as partially justified. The remaining 18 complaints were found to be unfounded. Comparing the total number of complaints to the previous year, it can be stated that the total number of complaints declined slightly.

Twenty complaints focused on the actions of the Public Relations Department, whose task is to deal with complaints and tips addressed to the Office. The vast majority of complaints were submitted by the complainant due to disagreement with the handling of their prior submission, which was set aside by the Public Relations Department without any measures taken. If a complainant submits a complaint pursuant to Article 175 of Act No. 500/2004 Coll., their prior submission and the manner by which it was dealt with by the given body are investigated. In the case of the Public Relations Department, the analytics unit assessed 2 complaints as justified and 6 as partially justified. The remaining 12 complaints were assessed to be groundless. In the case that reviewing the complainant's submission turned up a suspicion of violation of Act No. 101/2000 Coll., the legally stipulated procedure followed, with such

submissions being passed along either to an Office inspector for an inspection to be conducted or to the Administrative Department to launch administrative proceedings for suspicion of an administrative offence or misdemeanour.

In three cases the complainants turned to the Office with complaints against the actions of the Administrative Department. In all cases these complaints were found to be groundless.

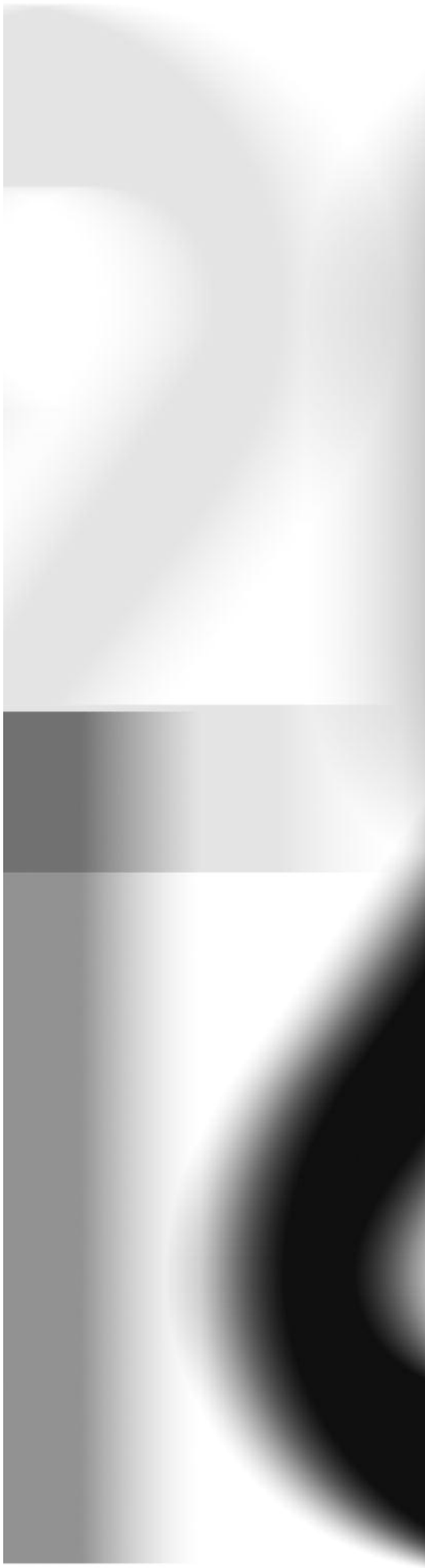
In ten cases the complainants turned to the Office with complaints against the conclusions of the Office's inspection procedures or actions by Office inspectors in leading an inspection. Of this number, 5 complaints were found to be partially justified and 3 were found groundless. In these cases the complainant was informed of the result of the investigation, any potential errors found and the further actions on the given matter. The Office received two complaints at the end of 2016 and will deal with them in 2017.

In all cases the relevant Office section was informed about the handling of the complaint and if its actions were found to be incorrect or partially incorrect it was called upon to adopt measures to prevent the same mistake from occurring again in similar cases.

In 2016 the Office received several complaints from entrepreneurs that domain name holders are handling their personal data as part of their activities without consent having been given. These personal data are identical to the data contained in the publicly accessible trade register. The public nature of certain data in the register, thus also broad availability on the internet, is laid down by Act No. 455/1991 Coll., on Trade Licensing (the Trade Licensing Act). In the case of copying personal data listed in the public part of the trade register and subsequent publishing on domains that do not damage the person and merely inform about businesses in the Czech Republic, these actions are not at odds with the legal title listed in Article 5(2)(d) of Act No. 101/2000 Coll., which allows the further processing of data lawfully published in accordance with special legislation, here the Trade Licensing Act. The Office, aware of the severity of the given problem, whereby the legal treatment opens up space for further processing and the commercial utilisation of data, sent comments to the coordinator of legislation on the Trade Register, the Ministry of Industry and Trade. The remarks included the text: "*The Office for Personal Data Protection has received a number of complaints from entrepreneurs about private law copies of the Trade Register that are indexed in internet search engines so that public access is provided to all identifying information on self-employed natural persons without having to make an intentional request, which would be the advisable thing. On the basis of private autonomy, i.e. that an entrepreneur is the owner of the data the public administration processes about them, it should be possible to opt out of such transfer of data. The most appropriate solution for newly registered businesspeople would seem to be a 'Robinson list' as per Article 5(9) of the Personal Data Protection Act, whereby an entrepreneur would be given the option upon registration of whether or not they want to allow their data to be transferred to the private sector. For existing entrepreneurs there would be a new opt-out request.*" There are even cases where these personal data of entrepreneurs are further used for commercial purposes. The Office is currently addressing this problem and analysing the legality of such actions.

As in the previous year, not one of the total of 33 complaints the Office received from complainants targeted inappropriate conduct of public officials. Based on this it is possible to state that the Office is professional in communicating with the public in handling all submissions received, its supervisory activity and in administrative proceedings while protecting their rights and legitimate interests.

Foreign Affairs and International Cooperation



In the area of international cooperation the Office concentrated primarily on activities under the Article 29 Working Party (WP29), which is an advisory body to the European Commission on issues of personal data protection. This year the Office decided to boost its direct representation in selected WP29 subgroups. Office specialists thus work in the following formations:

Cooperation subgroup – set up in association with preparations for the General Data Protection Regulation and deals with issues of future cooperation among authorities, which this Regulation will bolster by introducing new cooperation mechanisms, particularly in the field of dealing with complaints and investigating cases with an international aspect.

Technology subgroup – deals with the influence of new technology on individual privacy and their compliance with the personal data protection regulations.

International Transfers subgroup – deals with the issue of international data flow.

Borders, Travel and Law Enforcement subgroup – deals primarily with the influence of various security technologies and measures to protect personal data.

E-government subgroup – deals with issue of personal data protection during digitisation of state administration.

Key Provisions subgroup – works on legislative issues of moving from the current Directive 95/46/EC to the newly approved General Data Protection Regulation, which will replace it in May of 2018.

Aside from this the Office is represented directly by its President at the regular plenary sessions.

The Office also expanded bilateral cooperation with partner authorities. This was predominantly in the form of consultations on specific topics by correspondence. At the start of November, a two-day working meeting with representatives of the partner authority from Hungary took place in Prague. The talks focused on two main topics: free access to information versus

protection of personal data and practical steps for the period of shifting to the General Data Protection Regulation.

Aside from various one-off events, Office representatives took part in these selected international conferences organised annually:

- Meeting of authorities from Central and Eastern Europe – Sarajevo, May 2016 The programme included the topics of camera surveillance, protection of privacy in the workplace, and the processing of biometric data.
- Spring conference of data protection commissioners – Budapest, May 2016 The two-day meeting was dominated by the topic of the freshly approved General Data Protection Regulation.
- Seminar for swapping experiences from supervisory activity – Podgorica, October 2016 This event is traditionally focused on discussing practical findings from the field of inspection, dealing with complaints and sanctions.
- International Conference of Data Protection and Privacy Commissioners – Marrakesh, October 2016 The central theme was artificial intelligence and its impact on individual privacy.
- A specialist in legislation attended a two-day seminar on protection of personal data in the social security system as an instructor. The event, which was financed by the European Commission through its TAIEX office, took place in September in Ankara.

The Office, media and communication tools

From the perspective of media interest in the activities of the Office, 2016 had two main peaks. The first was associated with January's Position No. 1/2016 – Placement of Camera Systems in Residential Buildings. Based on its experience to date the Office re-evaluated and harmonised the conditions for camera surveillance in cases that do not cause serious problems and do not unduly invade privacy if the given rules are followed. Above all it was necessary to explain that making use of the basic legal grounds for making a camera recording in an apartment building, which is protection of rights and legitimate interests (protection of health, protection of property against theft) is not based on the consent of building residents with making and retention of a recording, i.e. to put it simply, an owners' association or housing cooperative does not need any consents in such a case. It must however fulfil the conditions listed in the position, in particular thorough securing of camera systems. Occasional misinterpretations appearing in the media were also effectively eliminated.

The second peak, which was associated with the greatest media interest, took place at the end of June with the launching of administrative proceedings with the company T-Mobile Czech Republic a.s. in connection with the theft of customer data. In these proceedings the Office stated that it considers it proven that the company as a controller of its clients' personal data failed to adopt sufficient measures to secure the personal data contained in the internal electronic database that contained the personal data of roughly 1.2 million customers – natural persons. As a result of failure to adopt sufficient measures, these data were stolen by one of the company's employees. The company thereby violated the obligation 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, thereby committing an administrative offence. In light of the nature of the case and the fine of CZK 3.6 million, making it the highest fine ever issued by the Office, it was presented to the public in lesser or greater detail by a truly broad range of media, be they print, audiovisual or electronic. This was done in a factual, informative manner.

Over the course of the year, the media registered other topics related to the Office or about which the Office had informed. This included for example the discussions around the amendment to the Act on Health Services, the issue of access to State Security archival materials, the Supreme Administrative Court decision on the e-bike case, and at the end of the year also the issue of Tax Numbers on EET (electronic records of sales) receipts. From a broader perspective of media interest in the issue of personal data protection we can mention in particular the new instrument for transferring data to the USA approved by the European Commission, the EU-US Privacy Shield. Last but not least, in May the European Union Official Journal published the General Data Protection Regulation, which the Czech Republic had been helping prepare since 2012 and which will take effect in the EU member states in May 2018.

SPREADING KNOWLEDGE ABOUT PERSONAL DATA PROTECTION

In May the Office organised an international conference in cooperation with the Charles University Faculty of Law on the topic of the right to informational self-determination, to which no independent conference had yet been devoted in the Czech Republic. This topic however is of quite fundamental significance in connection with the boom of modern information technology. In the opening speech, President of the Office for the Protection of Personal Data Dr Ivana Janů emphasised the importance of the conference, especially in developing the term "right to informational self-determination" and outlining the possible interpretations and approaches, particularly in the context of the current development of information technology and prepared changes to EU law to be brought about by the General Data Protection Regulation.

The topic of informational self-determination was dealt with from various points of view at the conference, in particular from the perspective of theory, case law and also practice. The quality of the international conference was ensured by the high standard of presenters. Dr Rolf Schwartmann from the Technical University of Cologne explained the term "right to informational self-determination" in the German legal code, while Dr Jiří Malenovský, a judge at the EU Court of Justice, presented on the topic of the right to informational self-determination and its expressions in the case law of the EU Court of Justice. The morning bloc was capped off by Dr Michael Ronellenfitsch, professor emeritus at the University of Tübingen, with a talk on German practice of the right to informational self-determination with special emphasis on the decision-making of the Federal Commissioner for Data Protection.

Round table on use of online cameras and other surveillance devices, 14 June 2016

February 2016 saw the end of two years of media cooperation under which nearly 50 articles and a number of video calling cards were published, the purpose of which was to increase awareness of personal data protection in various segments and react to the current communication needs of the Office at a time when greater awareness is being afforded to such issues as security. All the posts are also accessible on the Office's website in the section Media.

Experts from among the Office's employees gave lectures over the course of the year. This concerns a total of 25 presentations made at conferences or separate lectures in many different areas. A traditional topic was camera systems, but there were also lectures for municipal representatives, on the issue of data breaches, the field of healthcare, personal data protection in labour law and more.

Three Office Positions were issues and published on the website in 2016: the aforementioned Position No. 1/2016 – Placement of Camera Systems in Residential Buildings, and then Position No. 2/2016 – On the Processing of Personal Data of Participants during Provision of Financial Aid from the European Social Fund, and Position No. 3/2016 – Records of Visitors Entering Buildings and Copying of Documents. Two issues of the Office for Personal Data Protection Journal were issued (71 and 72).

The Office traditionally focused attention on children and youth as part of its public awareness activities. On the occasion of International Data Privacy Day, which is held on 28 January, it declared the 10th year of its youth competition "My Privacy! Don't Look, Don't Poke About!". The winners of two thematic and two age-based categories were invited to an award ceremony, where they received their awards from Office President Dr Ivana Janů.

Meeting with the winners of the 10th annual competition for children and youth "My Privacy! Don't Look, Don't Poke About!" accompanied by parents and teachers, 13 June 2016

On the occasion of the start of the new school year, the Office issued awareness pamphlets intended for children and youth, which are also available in electronic form on the website in the section For Youth. The fliers were distributed to interested primary and secondary schools from around the country. Cooperation was also established in this regard with Olomouc's Centre for Prevention of Risky Virtual Communication at Palacký University's Faculty of Education. The Office also became a partner of the 2016/2017 School Educational Diary, to which it contributed information on privacy and personal data protection. The diary was distributed to schools in a run of 15 000.

OFFICE LIBRARY

The Office Library totals 2300 volumes. It acts in part as support for employees (publications needed for their work are found here), but it is also available for the professional public for reference (whether for students or experts from the field) and following arrangements made by telephone it is possible to visit the library and study the needed materials there. In 2016, 82 new titles were added to the library, of those four as gifts.

OFFICE WEBSITE

A new section on the EU General Regulation was set up, in which all relevant information on the General Data Protection Regulation is and will continue to be added. Aside from the text of the Regulation and basic information about it, there is also an index to the General Regulation, a transfer table between the Act on Personal Data Protection and the General Data Protection Regulation and the contents of the Regulation. The contents of other selected legal regulations were also added to the website. A coherent overview with detailed information on inspections is newly been published in the section Supervisory Activity. A mobile version of the site is also being prepared, with a medium-term outlook to preparations for a responsive site.

Office Personnel

The number of job positions at the Office for Personal Data Protection is determined by the State Budget Act and the systemisation of service and job positions for the respective calendar year.

In 2016 the total number of systemised positions was 104.

Staff fluctuation in 2016 compared year-on-year rose slightly from 9% in the previous year to 9.8%.

In 2016 the launch of individual processes associated with civil service reform was gradually completed. At the start of 2016 the first service evaluation of civil servants assigned to serve at the Office for Personal Data Protection was conducted. Based on the service evaluations conducted, 18 civil servants were evaluated as excellent and 42 as good. No civil servant was evaluated as unsatisfactory. Six employees were brought in to serve in 2016, while 7 employees ended their service. Four new employees were employed in 2016 and 2 employees terminated their employment in 2016.

Seven applicants were tested as part of the civil service exam for the field of service in personal data protection provided by the Office; all passed the exam.

As of 1 January 2016, the records showed 101 employees at the Office; as of 31 December 2016 this number was 100.

The average registered number of employees for 2016 was 102.

A further 30 persons performed activities at the Office on the basis of concluded agreements on work performed outside employment.

According to the table "Breakdown of Office Employees by Age and Sex", employees at the Office are predominantly 50 years of age or 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.

The Office allows and provides for professional development of its employees. It ensures they can deepen their professional qualifications and if the Office so requires even increase them. It allows its employees to visit language courses and apply those language skills in carrying out their work or service. The Office provides the opportunity for secondary and post-secondary school students to complete internships, thereby supporting their interest in the issue of personal data protection while also seeking out new potential employees.

Breakdown of Office Employees by Age and Sex – as of 31 December 2016

Whole set	men	women	total
up to 20	0.00	0.00	0.00
from 21 to 30	3.00	8.00	11.00
from 31 to 40	9.00	13.00	22.00
from 41 to 50	6.00	6.00	12.00
from 51 to 60	12.00	19.00	31.00
61 and over	17.00	8.00	25.00
Total	47.00	54.00	101.00

Breakdown of Office Employees by Education and Sex – as of 31 December 2016

Whole set	men	women	total
C – Basic	0	1	1
H – Secondary technical + vocational certificate	1	1	2
J – Secondary technical	0	1	1
K – General complete secondary	2	4	6
L – Technical complete secondary + vocational certificate	1	2	3
M – Complete technical secondary	3	13	16
N – Higher technical education	0	2	2
R – Bachelor's	0	3	3
T – University	40	27	67
Total	47	54	101

Economic Management of the Office

The Office budget was approved by Act No. 400/2015 Coll., on the State Budget of the Czech Republic for 2016.

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

	in CZK thousands
Summary indicators	
Total income	6 475.91
Total expenditures	144 376.48
Specific indicators – income	
Total non-tax. capital income and accepted transfers	6 475.91
of which: total income from EU budget not including CAP	0.00
other non-tax and capital income and accepted transfers in total	6 475.91
Specific indicators – expenditures	
Expenditures to ensure performance of the tasks of the Office for Personal Data Protection	144 376.48
Cross-sectional expenditure indicators	
Employee salaries and other payments for work performed	50 743.61
Mandatory insurance premiums paid by the employer*)	17 053.23
Contribution to the Cultural and Social Needs Fund	744.23
Salaries of employees in an employment relationship in service positions	10 205.25
Salaries of employees in service positions under the Act on Civil Service	29 916.87
Salaries of employees derived from salaries of constitutional officials	9 410.15
Total expenditures co-financed from the EU budget not including CAP	0.00
of which: from the state budget	0.00
contribution from the EU budget	0.00
Total expenditures recorded in the information system for the EDS/SMVS funding programme	16 515.64

**) social security premiums and contributions to the state employment policy and public health insurance premiums*

1. Income

No income was set by the approved budget for 2016.

The income budget for Heading 343 – Office for Personal Data Protection was fulfilled with an amount of CZK 6 475 910.

These were primarily European Commission refunds for foreign trips by Office employees, sanctions imposed under Act No. 480/2004 Coll., on Certain Information Society Services, sanctions imposed under Act No. 101/2000 Coll., on Personal Data Protection, and under other laws, compensation for proceeding costs, revenue from the sale of a passenger car, revenue relating to 2015 (payment of remainder of deposit account for paying salaries and contributions to the Cultural and Social Needs Fund for December 2015).

Payment of imposed sanctions under the aforementioned acts were CZK 6 048 150, accepted non-capacity contributions and compensation related to previous years CZK 261 760, transfers from other own funds CZK 21 000 and revenue from the sale of tangible fixed assets CZK 145 000. All of the Office's income was transferred to the state budget.

2. Expenditures

Expenditure drawing of CZK 144 376 480 includes all costs for salaries and associated expenditures, capital expenditures associated with the Office building, renewal of fleet and information systems, both for the Office itself and the IS ORG. This also includes further current expenditures associated with operation of the Office, in particular items associated with the purchase of minor tangible assets, material, IT services, services associated with building operation and other services, travel expenses, training, maintenance and expenditures associated with non-investment purchases.

Expenditures for water, gas, electricity and fuel totalled CZK 1 924 730 in 2016.

The above amounts correspond to the requirement for efficient and economic operation of the Office.

3. Employee salaries and other payments for work performed, including associated expenses

Drawing of the budget for employee salaries, other expenses for work performed and associated expenses, including the Cultural and Social Needs Fund and compensation for sick leave, in the amount of CZK 68 694 520 corresponds to the qualification structure and meeting of the employee plan.

As of 31 December 2016 there were 102 employees.

4. Expenditures recorded in the Ministry of Finance programme financing information system – EDS/SMVS

In accordance with the approved documentation for Programme 143V01 "Development and Renewal of Material and Technical Base for Office for Personal Data Protection – From 2007", a total of CZK 16 515 640 was drawn.

Under the sub-programme 143V01100 "Acquisition, Renewal and Operation of Office ICT", a total of CZK 15 903 390 was drawn in 2016 in ***investment*** *systematically determined SR expenditures* for the following projects:

	in CZK thousands
project 143V011000063 "Extension of Enterprise contract for use of Microsoft products“	2 203,09
project 143V011000074 "Expansion of OPDP IS. cyber security“	2 709.16
project 143V011000075 "Modification of IS ORG-Phase 13“	1 907.67
project 143V011000076 "Renewal of central data storage"	2 939.30
project 143V011000077 "Modifications of Register module"	74.66
project 143V011000078 "Modifications of Tescoleg module"	69.45
project 143V011000080 "Modification of IS ORG-Phase 15“	544.50
project 143V011000082 "3.DB location and expansion of accessibility"	3 390.09
project 143V011000083 "Modification of IS ORG – Phase 16"	2 065.47

In sub-programme 143V01200 "Reproduction of OPDP Property" a total of CZK 612 250 was drawn in 2016 in ***investment*** *systematically designated SR expenditures* for the following projects:

project 143V012000020 "Building security – ISP system modifications)	89.40
project 143V012000021 "Renovation of apartment unit"	57.00
project 143V012002016 "Fleet renewal"	465.85

Overview of budget drawing in 2016

Budget structure type	Name of indicator	Approved 2016 budget in CZK thousands	Final 2016 budget in CZK thousands	Reality as per accounting statements as of 31 December 2016 in CZK thousands	Actual/ final budget in %
2211, 2212, 2324, 3113, 4132	Other non-tax income	0,00	0,00	6 475,91	
	TOTAL INCOME	**0,00**	**0,00**	**6 475,91**	
501	Salaries	48 760,09	49 710,44	49 532,27	99,64
5011	Salaries of employees in employment relation-ship with exception of employees in service positions	9 956,36	10 205,25	10 205,25	100,00
5013	Salaries of employees	29 218,13	29 919,59	29 916,87	99,99
	in service positions under the Act on Civil Service				

5014	Salaries of empl. derived from salaries of const. officials	9 585,60	9 585,60	9 410,15	98,17
502	Other payments for work performed	2 245,99	1 745,99	1 211,34	69,38
5021	Other personnel expenses	2 245,99	1 655,32	1 120,67	67,70
5024	Severance	0,00	90,67	90,67	100,00
503	Mand. insurance paid by employer	17 491,16	17 602,15	17 053,23	96,88
5031	Mand. social security premiums	12 751,52	12 833,13	12 503,81	97,43
5032	Mand. public health insurance	4 739,64	4 769,02	4 549,42	95,40
513	Purchase of material	1 595,00	1 858,00	1 579,11	84,98
514	Interest and other fin. expenses	15,00	45,00	41,55	92,34
515	Water, fuel and energy	2 400,00	1 982,86	1 924,73	97,07
516	Purchase of services	19 666,00	19 318,53	14 058,70	72,77
5169	Purchase of other services	8 242,00	6 806,41	5 298,80	77,85
517	Other purchases	37 587,33	44 657,90	38 821,72	86,93
5171	Repairs and maintenanc	35 248,33	42 008,91	37 111,313	88.34
5173	Travel expenses	1 700,00	1 925,00	1 270,78	66,01
518	Deposits, principal provided	330,00	540,00	0,00	0,00
519	Exp. assoc. w/ non-invest. purchases	2 904,60	2 885,71	2 725,55	94,45
5342	Transfers to CSNF	731,40	744,23	744,23	100,00
536	Other non-inv. transf. oth. pub. budg.	22,00	16,04	15,04	93,77
542	Compensation paid to pop.	200,00	200,00	153,44	76,72
5424	Compensation during illness	200,00	200,00	153,44	76,72
	Total current expenditures	**133 948,58**	**141 306,86**	**127 860,84**	**90,48**
611	Acquisition of fixed intangible assets	9 500,00	8 682,96	7 514,30	86,54
612	Acquisition of fixed tangible assets	8 200,00	10 704,29	9 001,34	84,09
	Total capital expenditures	**17 700,00**	**19 387,25**	**16 515,64**	**85,19**
	TOTAL EXPENDITURES	**151 648,58**	**160 694,11**	**144 376,48**	**89,85**

Numerical data used from reports drawn up as of 31 December 2016

INTERNAL AUDIT

(…)

FINANCIAL STATEMENT

Approval of the final financial statement for 2016 and information on its transfer will take place by the standard deadline of 31 July 2017 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 2016 a total of 53 requests for information were addressed to the Office, a slight decline compared to previous years. In many cases however extensive sets of information were requested concerning many spheres of the Office's activities and its area of jurisdiction, i.e. personal data protection.

The Office obliged 42 requests, in 3 cases it was forced to issue a decision on complete refusal to provide the requested information and 8 requests were partially rejected. The primary reason for partial or complete rejection was the protection of the personal data contained in the requested documents. Another reason for refusal was that the Office did not have the requested information at its disposal or such information did not exist, or it was information it had obtained from a third party while fulfilling supervisory activity tasks, or it was information related to criminal proceedings, the provision of which Act No. 106/1999 Coll. prohibits.

In one case an applicant filed an appeal against a decision on partial refusal to the President of the Office, who confirmed the first-instance decision. No complaints under Article 16a of Act No. 106/1999 Coll. against the Office's approach in handling complaints were submitted, nor was any court action launched in this regard.

The attention of applicants traditionally focused primarily on the decision-making practice of the Office, i.e. the results of administrative proceedings, the results of subsequent court proceedings and also the amount of sanctions imposed, or the summary thereof for previous years. A considerable number of requests focused on the Office's supervisory activity. Petitioners were provided with information on inspections carried out by Office inspectors at individual entities, on the results of these inspections and the corrective measures imposed. Areas where the interest of public was focused included the conditions of camera system operation and registration thereof, processing of vehicle identification numbers, etc.

Another group of requests related to the organisation of the Office, how its staff and funding is provided for, information systems used, as well as the results of financial control of the Office.

2016 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 2017.

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, 2017

ISBN 978-80-210-8507-7